Adriana Veloso Meireles

ALGORITMOS, PRIVACIDADE E DEMOCRACIA

Ou como o privado nunca foi tão político como no século XXI

Brasília, 2020.

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Va

Veloso Meireles, Adriana
Algorimos, privacidade e democracia; ou como o privado nunca foi tão político como no século XXI / Adriana Veloso Meireles; orientador Luis Felipe Miguel. -- Brasília, 2020.
174 p.

Tese (Doutorado - Doutorado em Ciência Política) -- Universidade de Brasília, 2020.

1. privacidade. 2. democracia. 3. algoritmos. 4. capitalismo de vigilância. 5. proteção de dados pessoais. I. Felipe Miguel, Luis, orient. II. Título.

BANCA EXAMINADORA:

Prof. Dr. Luis Felipe Miguel (IPOL/UnB) - Orientador

Prof. Dr. Rafael de Almeida Evangelista (Unicamp)

Prof. Dr. Danilo Cesar Maganhoto Doneda (IDP)

Profª. Dra. Marisa Von Bülow (IPOL/UnB)

Prof. Dr. Thiago Aparecido Trindade (suplente)

AGRADECIMENTOS

Gostaria de agradecer a todos amigos, familiares e colegas pelo estímulo e apoio ao longo dos quatro anos de desenvolvimento deste trabalho.

Sou muito grata a meu orientador, professor Luis Felipe Miguel, com quem aprendi muito e sem o qual este trabalho não seria realizado. Agradeço pela leitura sempre crítica e atenta, pelos ensinamentos em classe e durante a prática docente em que fui monitora. Agradeço pela confiança em realizar a tese.

Agradeço ao professores do Programa de Pós-graduação em Ciência Política do Instituto de Ciência Política (IPOL). À toda equipe do Ipol e a meus colegas de mestrado e doutorado pelos debates e reflexões.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), ao Decanato de Pesquisa e Pós-graduação (DPP/UnB), à equipe da Reitoria e Ouvidoria da Universidade de Brasília e à Fundação de Amparo à Pesquisa do Distrito Federal (FAP-DF), que possibilitaram minha dedicação à esta pesquisa e minha participação em eventos acadêmicos, fundamentais para o desenvolvimento do trabalho.

Aos membros da banca Profª Dra. Marisa Von Bülow, Prof. Dr. Rafael de Almeida Evangelista, Prof. Dr. Danilo Cesar Maganhoto Doneda e Prof. Dr. Thiago Aparecido Trindade pelas contribuições e observações sobre o trabalho. Ao Prof. Dr. Tiago Barros, que integrou a banca de qualificação da tese com sugestões de aperfeiçoamento.

Por fim, agradeço o amigo João S. O. Bueno pelas aulas de *Python* que resultaram no script da análise empírica.

Resumo

A tese analisou a relação entre a democracia, a privacidade e os algoritmos utilizando como fonte principal de investigação a literatura sobre estes temas e uma discussão empiricamente informada das sessões centrais do Fórum de Governança da Internet, principal evento internacional, realizado pelas Nações Unidas, para debater tecnologia e sociedade. O objetivo central do trabalho é mapear as principais controvérsias em torno do debate sobre privacidade e proteção de dados pessoais e sua relação com as democracias contemporâneas. A partir desta questão, examinou-se os principais marcos regulatórios que versam sobre o tema e como refletem princípios e valores democráticos. A metodologia de análise descreveu os procedimentos quantitativos e qualitativos adotados na pesquisa empírica e teórica. Dentre as principais conclusões do trabalho enfatiza-se a necessidade de regular o setor de tecnologia em questões que vão além da privacidade, em especial a forma como operam os algoritmos inteligentes.

Palavras chave: privacidade, algoritmos, proteção de dados pessoais, democracia, capitalismo de vigilância

Abstract

The thesis analyzed the relationship between democracy, privacy and algorithms using as main source of investigation the literature on these themes and an empirically informed discussion of the central sessions of the Internet Governance Forum, the main international event, held by the United Nations, to discuss technology and society. The main objective of the work is to map the main controversies surrounding the debate about privacy and protection of personal data and its relationship to contemporary democracies. From this question, the main regulatory frameworks that deal with the topic, and how they reflect democratic principles and values, were examined. The methodology described the quantitative and qualitative procedures adopted in the research both empirical and theorical. Among the main conclusions of the work, there is the need to regulate the technology sector in matters that go beyond privacy, especially the way in which intelligent algorithms operate.

Key words; privacy, algorithms, personal data protection, democracy, surveillance capitalism**.**

SUMÁRIO

LISTA DE FIGURAS

LISTA QUADROS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ANEXOS

Introdução

O campo de estudo sobre democracia digital, e-democracia, ciber democracia, ou até mesmo democracia eletrônica, surge na década de 1990 ancorado na expansão das tecnologias da informação e comunicação e nas possibilidades que os meios técnicos ofereciam para melhorar o sistema democrático liberal, como, por exemplo, a representação política, a participação, dentre outros aspectos. Autores destacavam o déficit deliberativo das democracias (Coleman e Blumler, 2009) para enfatizar como as ferramentas digitais poderiam operar como suporte para superar a crise das democracias representativas.

Ocorre que o próprio conceito de democracia, no campo da teoria política, está em constante disputa. Muito diferente de sua inspiração grega, os sistemas políticos de países considerados democráticos estão baseados em um sistema eleitoral, na representação política e na separação dos poderes. Após o final das duas grandes guerras mundiais observa-se uma certa hegemonia do entendimento que "o método democrático é aquele arranjo institucional para se chegar a decisões políticas no qual os indivíduos adquirem o poder de decidir através de uma luta competitiva para obter o voto do povo" (Schumpeter, 1976, p. 269). Estes sistemas incorporam em si uma contradição, pois "trata-se de um governo do povo no qual o povo não está presente no processo de tomada de decisões" (Miguel, 2014, p.13). Esta redução do ideal de democracia ao sistema eleitoral e representativo, adotada pela maioria dos países ocidentais, tem sua base em princípios formulados no final do século XVIII (Manin, 1995). Tal discrepância leva ao descrédito nas instituições e partidos políticos, a distância entre representantes e representados, a fluidez das preferências políticas, mas sobretudo um desacordo entre o ideal democrático e sua prática. Diante disso, emergem no campo da teoria política novas concepções e formulações sobre como as democracias contemporâneas poderiam superar estes desafios impostos pelo método eleitoral e pela representação política. O debate contemporâneo sobre as teorias da democracia será aprofundadas no primeiro capítulo do trabalho.

Em um primeiro momento, a partir da difusão das tecnologias da informação e comunicação, observa-se uma confiança nos meios técnicos para solucionar alguns dos problemas advindos do sistema eleitoral e representativo identificados pelas teorias da democracia. É dizer, ao associar o digital, ou eletrônico, ao conceito de democracia, há uma aposta nas tecnologias para minimizar o déficit de participação e os problemas de representação política que o sistema eleitoral impõe. As pesquisas e estudos sobre democracia digital privilegiaram as potencialidades que a Internet e as tecnologias proporcionaram para promover a participação social, o engajamento político, a redução da distância entre os representantes e representados, a aprimoração da prestação de contas por parte dos governos e políticos, dentre outras questões. Ferramentas de consultas públicas interativas,

deliberações online e propostas de democracia direta facilitada pelas tecnologias digitais foram destacadas como solução para problemas de representação política, *accountability* e participação (Meireles, 2015). De fato, em 2016, mais da metade das pesquisas na área de democracia digital tinha como foco a participação, ou a deliberação online. Outros temas identificados são a transparência e a divisão digital, além de estudos em teoria da democracia digital (Gomes, 2018, p. 68). Além destes estudos, deve-se considerar ainda aqueles que focam nos processos eleitorais e novas mídias.

Entretanto, estas pesquisas deixam de focar em um ponto central das tecnologias da informação e comunicação; a forma como operam os algoritmos, os softwares que fazem a interface de interação entre as pessoas e as máquinas. Com a vida cotidiana cada vez mais mediada por sistemas cibernéticos, torna-se crucial compreender a lógica de como operam e de que forma se relacionam com processos sociais, culturais e políticos. Neste contexto é importante destacar autores como Manovich (2001), que cunhou o termo estudos de software, e Castells (2001) que enfatizou como a sociedade em rede iria mudar diversos aspectos da vida em sociedade.

A questão central que a tecnologia digital introduz é a forma de armazenamento das informações. Computadores analógicos eram máquinas de cálculo que não geravam dados sobre seu uso, a não ser que fossem construídos dispositivos para esta finalidade. As máquinas digitais, por serem dispositivos cibernéticos, geram todo o tipo de informação a cada vez que são utilizadas, em processos complexos de retroalimentação. São tecnologias de comunicação e controle, no sentido de que são sistemas reguladores, que registram dados (Silveira, 2017; Snowden, 2019). Ocorre que, a partir da expansão da Internet e da computação pessoal, estes sistemas passam a catalogar informações sobre as pessoas que os utilizam. É neste contexto que Lyon (1994) problematizou como o registro das mais diversas interações no formato digital tinha o potencial de gerar amplos e sofisticados sistemas de vigilância.

Sendo assim, enquanto parte da teoria política saudava a Internet como meio de promoção de mais participação e novas práticas sociais, outra estava atenta a um silencioso fenômeno presente nas sociedades conectadas; a constante coleta e armazenamento de informações pessoais, que conforma a *big data*, fenômeno que se refere grandes volumes de dados. Estas abordagens enfatizam como o modelo de negócios dominante da Internet é baseado na coleta, armazenamento e tratamento de informações privadas, que são cedidas "voluntariamente" a partir dos termos de usos de sites e aplicativos, mascarada como forma de melhorar sua experiência de uso (Fernback e Papacharissi, 2007). Autores desta linha de pesquisa são responsáveis por cunhar conceitos tais como economia da intrusão (Silveira, 2016), economia da informação pessoal (Bruno, 2008) e capitalismo de vigilância (Zuboff, 2019). Tais estudos têm inspiração na sociedade disciplinar descrita por Foucault (2012), em que os espaços são moldados para a vigilância, ou seja, para exercer domínio sobre as pessoas. Outra grande influência é a sociedade de controle de Deleuze (1992), que já indica a descentralização

do modelo do panóptico de Bentham para uma vigilância diluída em toda a sociedade, ou seja, para além das construções e instituições. A conformação deste fenômeno será aprofundada ao longo do primeiro capítulo do trabalho.

Por fim, após introduzir o tema da democracia digital e dos algoritmos faz-se necessário associá-los à questão da privacidade, um conceito recente nas ciências sociais. Muitas vezes relacionado à noção da liberdade negativa, ou o direito de ser deixado em paz, a privacidade envolve ainda questões como a intimidade, a autonomia e o desenvolvimento da personalidade e da própria identidade. No contexto das sociedades liberais contemporâneas, marcadas pelo individualismo, a privacidade tornou-se o espaço do exercício da liberdade. Ocorre que, com a conformação do capitalismo de vigilância, em que há um monitoramento constante e automatizado das experiências individuais, a privacidade fica em suspenso, pois as informações pessoais são registradas, processadas a todo o tempo para finalidades pouco transparentes.

É neste contexto que o direito à privacidade deixa de ser suficiente para lidar com a quantidade de informações pessoais produzidas pela sociedade contemporânea (Doneda, 2006). O direito à proteção de dados pessoais emerge, portanto, para defender os indivíduos do uso indevido de suas informações, seja para fins de vigilância, como muitas vezes o tema é abordado, mas também para influenciar hábitos de consumo, preferências políticas, interferindo diretamente no exercício da cidadania e na autodeterminação informacional. A proteção de dados pessoais consolida um paradoxo das sociedades contemporâneas; a privacidade deixa de ser apenas um direito individual para tornar-se uma questão coletiva, de toda a sociedade interconectada. Os sistemas normativos que orientam a proteção de dados pessoais serão aprofundados no segundo capítulo do trabalho no qual se realiza uma análise comparativa entre a legislação da União Europeia, dos Estados Unidos e do Brasil.

Realizadas estas breves contextualizações acerca dos temas centrais do trabalho – democracia, privacidade e os algoritmos – enfatiza-se como este debate é relevante para a ciência política contemporânea, pois são fenômenos sociais que incidem diretamente no exercício da cidadania, de direitos e liberdades. Além disso, é uma discussão que está cada vez mais associada à processos políticos complexos, que envolvem tanto o modelo eleitoral e representativo, como novas formas de participação política e ativismo digital.

Portanto, o objetivo geral do trabalho é mapear as principais controvérsias em torno do debate sobre privacidade e proteção de dados pessoais e sua relação com as democracias contemporâneas. Sublinham-se ainda como objetivos específicos; 1) Debater o conceito de privacidade a partir da distinção público privado, estruturadora de modelos que pensam o mundo social, normas jurídicas e instituições; 2) Analisar como diferentes marcos regulatórios de proteção de dados pessoais refletem princípios e valores democráticos.

Para cumprir estas metas estabelecidas, parte-se de uma revisão da literatura sobre os

principais temas da tese; algoritmos, privacidade e teorias da democracia. O trabalho está dividido em quatro capítulos, além da presente introdução. Parte-se da contextualização da conformação do capitalismo de vigilância e como os algoritmos governam a vida cotidiana intermediada por dispositivos digitais. Em seguida, apresenta-se o debate sobre a dicotomia público privado nas ciências sociais, e como a conformação das democracias liberais é calcada na separação entre a esfera pública da privada. A partir de uma perspectiva histórica, demonstra-se que o exercício da liberdade e da cidadania se desloca da esfera pública para a privada. Neste contexto, debate-se como esta divisão se torna opaca com a proliferação das tecnologias da informação e comunicação, que desvincula ainda mais a metáfora espacial da distinção público/privado. A partir deste debate teórico atinge-se o objetivo específico do trabalho de discutir a distinção público privado, estruturadora de modelos que pensam o mundo social, normas jurídicas e instituições.

Na sequência, expõe-se como a privacidade surge como um privilégio de classe e de gênero, consolidando-se enquanto um direito ao longo das últimas décadas. Ao discutir dimensões da privacidade, retoma-se algumas questões associadas às teorias da democracia que são fundamentais para a compreensão do fenômeno do monitoramento automatizado das experiências privadas. Ao debater o conceito de autonomia dialoga-se com teorias da vigilância, que se ancoram na premissa de que os algoritmos atuam na modulação de comportamentos. A partir da problematização do behaviorismo radical, recorre-se ao debate teórico sobre o processo de formação das preferências, relações de poder, opressão e dominação. Além disso, é exposto como a falta de transparência sobre o funcionamento dos algoritmos revela a necessidade de sua regulação como complemento à própria proteção de dados pessoais.

Em seguida, apresenta-se o debate sobre transparência a partir de sua origem do conceito de publicidade. Ressalta-se que o termo surge associado à expansão do pensamento neoliberal, que impõe novas formas de governabilidade – ou governança – importando práticas administrativas à economia política. Neste contexto, discute-se ainda os dados abertos enquanto materialização da transparência digital e o modelo de governo aberto, uma retórica neoliberal, que busca sustentar este novo padrão de Estado a partir de valores democráticos, como a própria participação social e o exercício da cidadania, por meio da fiscalização dos governos.

Ainda no primeiro capítulo do trabalho, explora-se a dualidade entre privacidade e segurança, argumento recorrentemente utilizado para justificar a vigilância. Neste contexto, regata-se o debate sobre o contrato social, em que as pessoas renunciam a determinadas liberdades em troca de segurança. Confronta-se o contratualismo com problematizações colocadas pela teoria feminista, enfatizando os limites do consentimento. A partir dessa discussão teórica, discute-se seu paralelo digital; os termos de uso das plataformas de conteúdo e aplicativos digitais, contratos firmados entre as pessoas e as grandes corporações de tecnologia.

Por fim, para finalizar a revisão teórica da primeira parte do trabalho, debate-se o conceito de liberdade e sua relação com a privacidade. Aprofunda-se a crítica ao pensamento liberal e seus limites, apresentando teorias da democracia alternativas à hegemonia deste pensamento nas ciências sociais. Além disso, enfatiza-se como nas sociedades contemporâneas a privacidade torna-se condição para o exercício da liberdade de expressão, a própria cidadania e a participação política.

No segundo capítulo realiza-se uma análise comparativa dos principais marcos normativos que orientam as instituições e a sociedade sobre privacidade e proteção de dados pessoais. Parte-se dos principais aspectos do Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation*), legislação da União Europeia, em vigência desde 2018. Apresenta-se as principais definições associadas à proteção de dados pessoais e os princípios de proteção de dados. Descreve-se os direitos dos titulares de dados, as obrigações e reponsabilidades dos agentes de tratamento de dados e as sanções passíveis de aplicação, em caso de violação da legislação.

Em seguida, apresenta-se a abordagem estadunidense com relação à privacidade e proteção de dados. Composto por um conjunto de leis que, em sua maioria, envolvem questões dos direitos do consumidor e diretos da concorrência, os marcos normativos deste país orientam a atuação das principais empresas de tecnologia, identificadas pelo acrônimo FAMGA - Facebook, Amazon, Microsoft, Google e Apple. Posteriormente, apresenta-se uma análise da lei geral de proteção de dados brasileira, assim como suas alterações realizadas após aprovação pelo Congresso Nacional. O segundo capítulo é encerrado com quadro comparativo entre estes marcos normativos e suas principais diferenças.

Com este segundo capítulo, o objetivo específico do trabalho de exame de diferentes marcos regulatórios sobre privacidade e proteção de dados pessoais é parcialmente cumprido. Esta discussão servirá como base para a associação entre a legislação vigente e princípios democráticos, aprofundados na discussão empiricamente informada do terceiro capítulo.

Para ancorar o debate teórico na realidade empírica, propõe-se o recorte de análise das edições do Fórum de Governança da Internet, evento anual, realizado desde 2006, pela Organização das Nações Unidas, que reúne atores de diversos setores para debater governança da Internet e seus impactos nas sociedades e democracias. Para realizar a avaliação serão utilizados métodos combinatórios quantitativos e qualitativos com vistas a mapear as principais controvérsias em torno dos debates sobre privacidade e proteção de dados pessoais (Latour, 2012; Denzin e Lincoln, 2011; Babbie, 2015). Os dados analisados serão as transcrições das atividades do Fórum, disponibilizadas em seu website[1]. A partir de uma avaliação quantitativa, em que se identificou palavras chave da pesquisa – privacidade, vigilância, segurança, liberdade e direitos – é realizada um exame dos

[1] Internet Governance Forum. Disponível em https://www.intgovforum.org/multilingual/. Acesso em 23/12/19.

discursos mobilizados em torno destes temas e como refletem visões distintas de valores e princípios democráticos.

Neste terceiro capítulo apresenta-se a metodologia utilizada, os procedimentos e técnicas adotados para cumprir com o objetivo geral de mapear as principais controvérsias em torno do debate sobre privacidade e proteção de dados pessoais e sua relação com as democracias contemporâneas. A partir da análise dos discursos mobilizados durante as edições do Fórum de Governança da Internet, identifica-se as principais controvérsias em torno da privacidade e proteção de dados pessoais, assim como as visões de democracia mobilizadas em torno destes argumentos. Apresenta-se os resultados quantitativos e qualitativos da discussão empiricamente informada aprofundando nas principais controvérsias identificadas em um quadro de sua evolução histórica. Com isto, complementa-se o objetivo específico de analisar como diferentes marcos regulatórios de proteção de dados pessoais refletem princípios e valores democráticos.

O presente trabalho busca contribuir com a discussão teórica sobre a separação das esferas em seu contexto atual em que metade da população mundial tem acesso às tecnologias da informação e comunicação. O debate realizado sobre privacidade subsidia a argumentação sobre a proteção de dados pessoais e seu aspecto coletivo. Outra contribuição do trabalho é a análise comparativa dos diferentes marcos regulatórios que versam sobre o tema e como eles refletem valores democráticos. Por fim, a partir da discussão empírica em que adotou-se uma metodologia combinatória quantitativa e qualitativa o trabalho cooperou para mapear a evolução das principais controvérsias que envolvem o setor de tecnologia.

Nas considerações finais, as conclusões do trabalho são apresentadas a partir do debate teórico e a análise empírica sobre os argumentos mobilizados em torno da discussão sobre privacidade e proteção de dados pessoais no âmbito do Fórum de Governança da Internet. Identifica-se a dificuldade do Estado em normatizar o setor de tecnologia e como sua auto regulação aprofundou questões como o próprio capitalismo de vigilância e outras, como o fenômeno do discurso de ódio e a desinformação. A partir deste debate, identificou-se outra grande controvérsia presente nos debates sobre privacidade e proteção de dados pessoais; a questão da remoção de conteúdo online. A partir desta problematização, resgata-se o argumento sobre a necessidade de regulação dos próprios algoritmos, considerada uma abordagem mais efetiva e com menor impacto no exercício da liberdade de expressão. Neste contexto, ressalta-se como o modelo de licenciamento dos algoritmos deve modificar-se para atender aos interessas das sociedades e não das empresas. Por fim, destaca-se a diferença dos impactos destes fenômenos em sociedades do norte e sul global, com ênfase para o fenômeno do colonialismo digital.

A presente introdução contextualizou e justificou a relevância do debate sobre privacidade e proteção de dados pessoais para a ciência política contemporânea, enquanto um problema social e

coletivo, que ultrapassa a garantia do exercício de direitos por parte do Estado. Apontou-se o referencial teórico que será trabalhado nos próximos capítulos, os objetivos da tese e a metodologia utilizada para que as metas da pesquisa sejam cumpridas.

1 – Algoritmos, web e capitalismo de vigilância

Este primeiro capítulo abordará os três temas centrais do trabalho; os algoritmos, a privacidade e as teorias da democracia relevantes para contextualizar o debate proposto. Inicia-se a partir da caracterização da passagem do modelo analógico ao digital e a consolidação das tecnologias da informação e comunicação nas sociedades contemporâneas. Neste contexto enfatiza-se como os algoritmos tornaram-se onipresentes nos sistemas cibernéticos e como sua forma de funcionamento é opaca. Descreve-se como em pouco menos de vinte anos o fenômeno do monitoramento automatizado das experiências privadas, realizado por algoritmos inteligentes com a intenção de induzir consumos e comportamentos se estabiliza, sendo conceituado como capitalismo de vigilância (Zuboff, 2019). São discutidos os impactos destes fatos na sociedade, em especial em como afetam o exercício da cidadania, a participação democrática e a reprodução de desigualdades.

Na segunda parte do capítulo parte-se da dicotomia público privado para introduzir o debate sobre a privacidade, em especial diante da expansão das tecnologias da informação e comunicação e da cultura do compartilhamento. A partir do histórico da distinção entre público e privado, que embora seja alvo de críticas, é estruturador de diversos modelos do mundo social, debate-se como a Internet torna esta divisão opaca e, sobretudo expõe que é preciso desvincular a metáfora espacial que fixa estas esferas como predeterminadas. Ao longo do debate sobre a divisão sobre público e privado problematiza-se a conformação do espaço público e o próprio conceito de democracia, alvo de disputa de diferentes correntes da teoria. Contextualiza-se o pensamento liberal para em seguida contrapô-lo a outras correntes das teorias da democracia.

Em seguida, são debatidos tanto o conceito de privacidade como suas diversas dimensões. Recorre-se ao modelo de integridade contextual para enfatizar a necessidade de controle sobre as próprias informações nos ambientes digitais. Debate-se ainda características da expressão online, em especial por meio das mídias sociais. Neste contexto demonstra-se que a cultura do compartilhamento é antagônica à privacidade e colabora para a consolidação do fenômeno do monitoramento automatizado de experiências pessoais, que se tornam o eixo central do mercado de dados pessoais.

Por fim, ao explorar dimensões da privacidade, tais como a autonomia, a transparência, a segurança e liberdade, são debatidos problemas fundamentais da ciência política contemporânea como o contratualismo, a dominação e o exercício do poder, o papel do Estado, a expansão do neoliberalismo, a liberdade de expressão e o exercício da cidadania. Com isto apresenta-se os conceitos centrais que orientam as próximas etapas do trabalho; a avaliação normativa da regulação de proteção de dados pessoais, a análise empírica sobre os discursos mobilizados em torno do tema da privacidade ao longo de treze anos do Fórum de Governança da Internet e quais as principais controvérsias associadas à diferentes visões de democracia identificadas.

A seguir contextualiza-se a passagem do analógico ao digital e como os algoritmos se tornaram onipresentes, desempenhando papel central na conformação do capitalismo de vigilância e no próprio funcionamento da Internet, da web e dos aplicativos digitais. Entretanto, não são uma novidade da era moderna, pois identifica-se seu uso nas antigas Grécia e Pérsia. O ponto central é que a forma de registro das informações transforma-se radicalmente na passagem do analógico para o digital. Na era moderna Ada Lovelace é considerada a primeira autora de um software, ou uma sequência de instruções escritas para serem interpretadas por um computador. Ela foi responsável por escrever o primeiro algoritmo a ser processado por uma máquina, no caso a máquina analítica de Charles Babbage, em 1843 (Barbrook, 2009). Entretanto, levaria ainda quase um século para que o primeiro computador moderno fosse construído. Em 1936, Alan Turing publicou um artigo em que conceituava algoritmos e um modelo abstrato de computador, a máquina universal. Dez anos se passariam até que de fato fossem construídas as primeiras máquinas com o objetivo de realizar cálculos para a Segunda Guerra Mundial. Tanto o britânico *Colossus*, como o americano ENIAC (*Electronic Numerical Integrator and Computer*) datam de 1943 (Barbrook, 2009).

A própria origem da Internet tem uma relação direta com a guerra, já que a Agência de Projetos de Pesquisa Avançada de Defesa (ARPA), responsável pela primeira Internet, foi fundada em meio à Guerra Fria, em 1958. No início da década de 1970, o primeiro e-mail foi enviado pela Arpanet, introduzindo o símbolo @. Em 1973, é lançado o Xerox Alto, considerado o primeiro computador de mesa (*desktop*), responsável por introduzir boa parte das metáforas utilizadas na computação pessoal, como mesa de trabalho, lixeira, pastas, dentre outras.

Já a década de 1980 ficou marcada pela Internet discada e a chegada de novos competidores da computação pessoal. O Apple Lisa é lançado em 1983, e dois anos depois, surge a primeira versão do Windows, da Microsoft. É nesta época que é publicado o Manifesto GNU[2], um convite à comunidade técnica para desenvolver um sistema operacional alternativo às opções comerciais. As atualizações do manifesto GNU viriam a cunhar o termo *copyleft*, um trocadilho com o termo de direitos autorais *copyright.* Assim, o manifesto introduz a licença GPL, que é baseada em quatro liberdades aos usuários de software; executar, acessar e modificar o código fonte dos programas e redistribuir cópias, com ou sem modificações.

O software livre, portanto, possui o código aberto, mas nem todo sistema de código aberto é um software livre (e o sistema operacional Android do Google é um exemplo, dentre vários). O fato de um sistema possuir o código aberto não tem implicações sobre sua forma de distribuição, definida a partir da licença de uso. É a licença que diferencia o software livre dos sistemas de código aberto, caracterizados pela aproximação com o setor privado. Portanto, o software livre está calcado na

[2] Manifesto GNU. Disponível em <https://www.gnu.org/gnu/manifesto.pt-br.html>. Acesso em 12/10/10.

liberdade de uso e distribuição, o que modifica toda a lógica de direitos autorais da indústria cultural.

Ainda durante a década de 1980 ocorre a transição da Arpanet para a Internet. O processo é liderado pelo cientista da computação John Postel, que editou os *Request for Comments* (RFC; em português, "pedido de comentários"), documentos técnicos responsáveis pela padronização de protocolos essenciais para o funcionamento da rede. Ele administrou a *Internet Assigned Numbers Authority* (IANA) até sua morte em 1998, contribuindo para que a gestão da Internet passasse do Departamento de Defesa dos Estados Unidos para o Departamento de Comércio do país, sendo operada por meio da *Internet Corporation for Assigned Names and Numbers* (ICANN).

Entretanto, é apenas no final de 1990 que a Internet se torna web. Tim Berners Lee publica os protocolos WWW (World Wide Web) e o HTTP (*Hypertext Transfer Protocol*, em português Protocolo de Transferência de Hipertexto) que basicamente cria todo o sistema hipermídia, de links e audiovisual presentes na interação das páginas da Internet. Neste mesmo ano de 1990, a Arpanet é fechada, abrindo espaço para a constituição da Internet e da web. É importante destacar que, apesar do senso comum sempre falar em Internet, é a web que conecta as pessoas e torna os conteúdos públicos. Uma metáfora que ilustra esta diferença é a dos trilhos – Internet – e os trens – a web. É esta última que transporta e conecta as pessoas, com base em uma infraestrutura anterior. A Internet é a primeira camada da rede constituída por servidores, os provedores de serviço, pontos de troca de tráfego (PPTs) que constituem a espinha dorsal – conhecida como *backbone* – da rede.

Enquanto isso, no Brasil, precisamente um mês antes da promulgação da Constituição de 1988, o país finalmente se conectava à Internet, ou melhor, à *Bitnet* (*Because It's Time Network*) por meio da iniciativa conjunta de professores da Fapesp (Fundação de Amparo à Pesquisa do Estado de São Paulo) e Universidade Federal do Rio de Janeiro (UFRJ). No final da década de 1980, é criada a Rede Nacional de Ensino e Pesquisa (RNP), que em 1991 começou a implementar o primeiro *backbone* brasileiro. Em 1995 é criado o Comitê Gestor da Internet do Brasil (CGI.br), órgão multissetorial responsável pela governança da Internet no país. Sua composição agrega membros do setor governamental, privado, comunidade cientifica e tecnológica e representantes do terceiro setor. Também em 1995 a estatal Embratel começa a oferecer o serviço de Internet comercial.

Durante a década de 1990, o acesso à Internet e a computação pessoal se amplia nos grandes centros urbanos. A partir da criação da web se multiplicam os conteúdos online e o compartilhamento de informações, softwares, músicas, dentre outros conteúdos. O projeto GNU ganha um importante colaborador, que desenvolve o núcleo de um sistema operacional – o Linux – e o coloca disponível na web, tornando possível assim softwares livres em computadores pessoais. É neste contexto que nos Estados Unidos é aprovado, em 1998, o *Copyright Term Extension Act*, que ampliou as regras de direitos autorais para os softwares, protegendo o setor de tecnologia. Surge assim a noção de pirataria de software, ou seja, a reprodução não autorizada.

Ainda em 1998, o Google é lançado por dois estudantes de universidade de Stanford, Larry Page e Sergey Brin. A ferramenta de buscas, à época, se destacou dos concorrentes por uma série de motivos. O mais perceptível deles era seu aspecto visual, que contava com um design minimalista, ou seja, apresentava poucas informações na página, ao contrário de seus rivais, Altavista, Yahoo!, dentre outros. Aliado a isso, a ferramenta era conhecida por não promover anúncios de forma ostensiva, como a concorrência. A empresa se propunha a "organizar as informações do mundo para que sejam universalmente acessíveis e úteis para todos[3]". Na prática se propunha a indexar a web.

Nos primeiros anos a companhia estabeleceu uma relação com as pessoas que utilizavam a ferramenta de busca que não era baseada no consumo, mas na experiência de uso - *user experience* em inglês (Saffer, 2010). Foi pioneira em investir na experiência do usuário, que aliado ao conceito de usabilidade formam o campo do design de interação (Moggridge, 2006; Preece *et all*, 2005). A usabilidade analisa sistemas e produtos de forma objetiva a partir de critérios específicos, tais como visibilidade, consistência e padrões, prevenção de erros, uso de metáforas, dentre outros (Nielsen, 1994). Por sua vez, a *user experience,* aproxima-se do design emocional, ou seja, a relação que as pessoas estabelecem com os produtos, um campo bem mais subjetivo (Norman, 2008).

Inicialmente, a empresa utilizava os dados - palavras chave, padrões de termos de pesquisa, como uma consulta é feita, ortografia, pontuação, tempos de permanência nas páginas, padrões de cliques, localização, dentre outros - exclusivamente para melhorar a ferramenta de busca e a experiência das pessoas ao utilizá-la. Estas informações adjacentes alimentavam o algoritmo do Google, em um "processo reflexivo de aprendizagem e melhoria contínua" (Zuboff, 2019, p.70). Quanto mais as pessoas utilizavam o buscador, mais relevantes tornavam-se os resultados procurados.

O Google investia a sabedoria adquirida sobre os padrões de navegação, cliques e todo o comportamento das pessoas em sua página para melhorar sua ferramenta e desenvolver outros serviços, como por exemplo a tradução. Nos anos iniciais, estas informações comportamentais não eram utilizadas de forma comercial, apenas como um conhecimento sobre o público, que era investido para melhorar o próprio produto. Entretanto estes "dados excedentes" eram armazenados pelo algoritmo do buscador, conhecido como *PageRank* (Page e Brin, 1998). Inicialmente este código era simples, mas na medida em que foi aprendendo com a experiência das pessoas começou a se tornar "inteligente".

No final da década de 1990, ocorreu o fenômeno que ficou conhecido como a bolha da Internet, ou das companhias ponto com. Em resumo, ocorreu uma grande especulação em torno das empresas de tecnologia, que obtiveram um pico de alta em suas ações na bolsa de valores Nasdaq, seguido de uma queda brutal. A decaída dos investimentos levou muitas empresas de tecnologia à

[3] Sobre o Google. Disponível em https://about.google/. Acessado em 7/2/19.

falência, venda, fusão, ou simplesmente o desaparecimento. Zuboff (2019) narra que os fundadores do Google tinham pavor de se tornarem um Nicola Tesla do novo milênio, em referência ao inventor contemporâneo de Thomas Edison, que morreu sem ser reconhecido. É neste contexto de pressão, que os fundadores da empresa transformam o negócio de um simples buscador destinado a organizar a informação da *web*, para entrar no ramo dos e-mails, textos, fotos, vídeos, geolocalização, reconhecimento facial, identificação de epidemias, carros autônomos, mapeamento da lua, entre outras atividades incorporadas pela *Alphabet*, fundada por eles em 2015.

Em primeiro lugar, renunciam a uma das regras que haviam adotado até então; a ausência de anúncios. Inicialmente, Page e Brin acreditavam que a presença de publicidade na ferramenta de busca levaria a seu descrédito e, por isso, eram resistentes à sua implementação. O *Adword* é lançado em 2000, em um modelo de negócios que os anunciantes pagavam mensalmente para que a empresa os promovesse. Nos primeiros anos "a equipe de anúncios consistia em sete pessoas, que em sua maioria compartilhavam a antipatia geral dos fundadores com relação aos anúncios" (Zuboff, 2019, p. 72). A transformação ocorre a partir de 2002, quando reformulam a ferramenta de anúncios *Adword*. "Se era para ter propaganda, ela deveria ser relevante para os usuários. A publicidade deveria aparecer (...) de uma forma direcionada a um indivíduo em particular (…), garantindo assim a relevância para as pessoas e o valor para os anunciantes" (Zuboff, 2019, p. 75). É a partir daí que o Google transforma a forma de monetizar a publicidade online, criando taxas de conversão baseadas, ou na quantidade de cliques, ou de visualizações, ao invés de uma mensalidade fixa.

O surgimento do marketing direcionado promovido pelo Google tem como fundamento uma vantagem mercadológica incontestável; o conhecimento prévio sobre a forma com que as pessoas realizavam buscas em sua ferramenta. Todas as informações que, antes eram aplicadas às melhorias do buscador, estavam agora disponíveis para promover os anunciantes. Os dados comportamentais antes utilizados para melhorar a experiência dos usuários alimentaram os algoritmos da empresa ao longo dos anos. Uma experiência acumulada de quase cinco anos e bilhões de dados. Para Zuboff (2019), esta mudança na forma de anunciar é um dos elementos que marcam o início do que ela define como o capitalismo de vigilância, conceituado pela autora como "uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas" (p.1). Compreende-se este fenômeno também como o monitoramento automatizado das experiências privadas, realizado por algoritmos inteligentes com a intenção de induzir consumos e comportamentos, conceitos que serão retomados ao longo do trabalho.

Ainda em 2002, uma inesperada busca dá indícios ao Google de que seu algoritmo estava aprendendo, ou se tornando inteligente. Zuboff (2019) destaca como um momento chave para o desenvolvimento dos algoritmos da empresa o caso da atriz Carol Brady. A autora narra como os engenheiros da empresa ficaram surpresos com o aumento das buscas sobre o nome dessa quase

desconhecida atriz americana. Até que identificaram que havia uma pergunta a seu respeito no programa "Quem quer ser um milionário". A partir da análise de dados verificaram como as buscas ocorriam de forma geolocalizada, ou seja, associando o fuso horário das regiões em que o programa ia ao ar na TV. O caso despertou a atenção dos desenvolvedores da empresa para "o poder preditivo da ferramenta, capaz de revelar eventos e tendências antes que eles entrassem no radar da mídia tradicional" (Zuboff, 2019, p.37). Em 2009, durante a pandemia da gripe H1N1, o Google revelou um experimento semelhante que foi amplamente documentado (Tutt, 2017). O Centros de Controle e Prevenção de Doenças do governo americano estavam detectando o avanço da doença com duas semanas de atraso, devido à demora das pessoas em buscar um médico após infectadas (Tutt, 2017). Com uma massiva base de dados, somada a um algoritmo que identificava palavras chave relacionando-as ao local da busca, o Google conseguiu identificar onde estavam os surtos de H1N1 em tempo real (Tutt, 2017). Essa não foi a primeira vez que a corporação iria cooperar com o governo.

Em 2003, o Google começa a desenvolver e implantar algoritmos de inteligência artificial, que, apesar de serem matemática pura, estão longe de possuírem um caráter neutro, assim como outras tecnologias. Neste mesmo ano, quatro engenheiros da empresa submetem uma patente intitulada "Gerando Informação sobre o usuário para utilização em publicidade direcionada" (*Generating User Information for Use in Targeted Advertising*)[4]. Em sua descrição, elencam uma série de maneiras para gerar informações de perfil de usuário (*user profile information*, ou UPI). Importante ressaltar que em 2003, o Google ainda era apenas uma ferramenta de busca. Não havia o Gmail, tampouco uma conta para entrar. As informações eram coletadas a parir dos endereços I.P. e ferramentas simples como os cookies. Para Zuboff (2019), esta patente representa o momento que o marketing deixa de ser um campo de estudo da comunicação, estudos de mercado, dentre outros, e passa a integrar uma ciência bastante exata; a matemática.

Esta patente posteriormente ficou conhecida como o *Adsense*, uma evolução do *Adwords*. A partir da "análise semântica e capacidades de inteligência artificial" (Zuboff, 2019, p. 84) o Google expandiu sua capacidade de extração de dados para todas as páginas da web, sendo capaz de ampliar os destinos publicitários para além de seu mecanismo de buscas. Essa mudança na forma de vender anúncios fica conhecida como a "física dos cliques" e segue como a principal fonte de lucro da empresa. O ano de 2003 é especialmente relevante devido a outros motivos, mas principalmente pela aproximação das agências de segurança estadunidenses com a empresa. É neste ano que o Google é contratado[5] pela Agência Central de Inteligência (CIA) "para customizar uma ferramenta de busca

[4] Generating user information for use in targeted advertising. Disponível em https://patents.google.com/patent/US20050131762A1/en. Acessado em 7/2/19.
[5] Exclusive: Google, CIA invest in 'future' of web monitoring. Disponível em https://www.wired.com/2010/07/exclusive-google-cia/. Acessado em 7/2/19.

(...) para supervisionar informações super secretas, secretas, sensíveis e não classificadas para ela e outras agências" (Zuboff, 2019, p. 84). A Agência Nacional de Segurança (NSA), por sua vez, pagou à empresa mais dois milhões de dólares para "buscar um algoritmo capaz de pesquisar quinze milhões de documentos em vinte e quatro idiomas[6]" (Zuboff, 2019, p.84). Estes dois contratos são o início de uma colaboração sem precedentes entre a empresa e o governo, que constituem a base do capitalismo de vigilância.

Por isso, a parceria continuou nos anos seguintes. Em 2004, o Google comprou a empresa *Keyhole*, que havia recebido investimentos da CIA para o mapeamento geográfico do planeta. O resultado foi o lançamento do Google Maps e do *Street View*, no ano seguinte. Esta colaboração entre o governo estadunidense e o Google é considerada sem precedentes e se caracteriza pela lógica neoliberal; ou seja, o Estado atua como protetor da concorrência em vez de atuar na proteção de direitos sociais e na busca pela igualdade (Harvey, 2008; Brown, 2015; Fraser 2012; Dardot e Laval, 2016). Havia uma demanda para a defesa de ameaças de segurança na Internet e o Vale do Silício continha o desenvolvimento tecnológico que o governo necessitava (Zuboff, 2019). Estes são apenas os primeiros exemplos dessa parceria, que seriam expostos pelas revelações de Edward Snowden sobre a vigilância em massa, em 2013[7].

Esta colaboração entre o financiamento governamental e o desenvolvimento tecnológico realizado por agentes privados fez com que os esforços regulatórios fossem mínimos, tema aprofundado no segundo capítulo do trabalho. Cada tentativa de regular o mercado de tecnologia era rebatida pelas empresas como uma forma de inibir a inovação (Bork e Sidak, 2012). Neste contexto, tanto o setor privado estava à vontade para explorar novas tecnologias, como o governo não tinha interesse em frustrar o desenvolvimento, que lhe fornecia as ferramentas de vigilância e monitoramento em nome do combate ao terrorismo. Este arranjo neoliberal é o início da expansão do poder corporativo e do capital financeiro, que se fundiria com o setor de tecnologia ao longo dos anos, já que muitas delas são controladas diretamente por grupos de investidores (Dantas, 2019). Este fato se torna ainda mais relevante quando se observa que os donos das empresas de tecnologia estão entre os empresários mais ricos do mundo[8]. De fato, as FAMGA – Facebook, Apple, Microsoft, Google e Amazon – são conhecidas por realizaram um forte *lobby* junto ao governo estadunidense contra a regulação da proteção de dados pessoais e a privacidade[9].

Um exemplo de como o Google transformou a percepção cultural e política é o Gmail, lançado

---

[6] Google and the US government. Disponível em http://insidegoogle.com/wp-content/uploads/2011/01/GOOGGovfinal012411.pdf. Acessado em 7/2/19.
[7] The NSA files. Disponível em < https://www.theguardian.com/us-news/the-nsa-files>. Acesso em 23/10/19.
[8] The World's Billionaires. Disponível em https://www.forbes.com/billionaires/list/#version:static. Acessado em 7/2/19.
[9] Google, Amazon, and Facebook all spent record amounts last year lobbying the US government. Disponível em https://www.recode.net/2019/1/23/18194328/google-amazon-facebook-lobby-record. Acessado em 7/2/19.

em 2004. No ordenamento liberal o princípio do sigilo postal é imprescindível e justamente por isso, "quando a ferramenta de e-mail da empresa foi lançada gerando anúncios a partir da leitura automatizada de correspondências privadas causou uma forte reação pública" (Zuboff, 2019, p. 51). A despeito da diferença de meios – papel, envelope e carteiro de um lado, teclado, tela e fibra ótica do outro –, correio convencional e correio eletrônico cumprem exatamente o mesmo propósito. O fato de que o sigilo das mensagens seja dispensado revela o declínio da noção de privacidade, tema que será aprofundado na segunda parte deste capítulo.

Para Zuboff (2019), o capitalismo de vigilância se consolida a partir de três fenômenos sociais; a liberdade em explorar um amplo conhecimento sobre o público sem sofrer interferências, os usuários transformam-se em consumidores e recursos e, por fim, há uma indiferença radical com relação aos valores democráticos (p.354). Os dois primeiros estão silenciosamente associados; enquanto as pessoas ignoram de que forma suas informações pessoais são tratadas, estes dados são os recursos necessários para o mercado de dados. É esta convergência sem precedentes entre liberdade e conhecimento, que fundamenta o modelo de negócios baseado nos dados pessoais. O dado pessoal passa a ter uma tripla natureza; refere-se ao indivíduo, sustenta a construção de políticas públicas, mas também é a essência do capitalismo de vigilância. Portanto, a regulação da propriedade dos dados é uma das questões contemporâneas mais complexas que a sociedade enfrenta, diante do tratamento indiscriminado de informações pessoais.

A indiferença radical com relação aos valores democráticos pode ser observada a partir do abandono da reciprocidade orgânica com as pessoas, que já não são apenas consumidores, mas também fonte de material bruto para o desenvolvimento de produtos personalizados. Além disso, Zuboff (2019) ressalta que as empresas de tecnologia empregam menos trabalhadores se comparadas com outros setores da economia, retirando o que ela considera como um balanço secular entre o capitalismo de mercado e as democracias contemporâneas. A autora destaca que "a General Motors empregou mais pessoas durante o pico da Grande Depressão do que o Google e Facebook contratam juntos atualmente" (Zuboff, 2019, p.468). A comparação entre 1929 e 2019 demonstra a erosão do modelo em que a economia prevalece sobre a política, que leva à consolidação do neoliberalismo e a concentração de renda.

Sendo assim, Zuboff (2019) ressalta que "a ausência de reciprocidade orgânica com as pessoas, seja enquanto elas sejam fonte enquanto consumidoras ou como trabalhadores é uma questão de importância excepcional à luz da relação histórica entre o capitalismo de mercado e a democracia" (p. 469). Isto ocorre devido à privatização da liberdade e do conhecimento, ou seja, não é mais o Estado que detém as informações e a capacidade de impor limites ao livre mercado. A indiferença radical com a visão coletivista da sociedade ainda é observada quando o conteúdo da informação é julgado pelas empresas a partir de sua relevância em termos de números de cliques e curtidas, volume,

profundidade e capacidade de gerar lucro (Zuboff, 2019, p. 472). Não importa se o conteúdo é mentiroso, fraudulento, ou contém discurso de ódio. Os valores democráticos são ignorados para sustentar o sistema financeiro e corporações de tecnologia e o Estado autua na defesa de interesses privados em detrimento dos coletivos.

A temática sobre o fluxo e os filtros de conteúdo na web será recorrente no debate sobre privacidade e liberdade de expressão, aprofundado na segunda parte deste capítulo. Por quanto é importante destacar que, para Zuboff (2019) o "principal desafio para a indiferença radical é a tentativa de substituir o jornalismo na Internet, quando as plataformas se colocam entre as publicações e a população, sujeitando o conteúdo jornalístico à mesma categoria de outros tipos de conteúdo" (p. 473). O reflexo mais direto desta investida é a propagação das notícias falsas, outro tema que será continuamente debatido. Por enquanto, ressalta-se que Zuboff (2019) enfatiza outros exemplos em que a desinformação prevaleceu sob imperativos econômicos, implicando diretamente nas relações de consumo e contratos assimétricos.

Dentre eles, a autora destaca uma multa de 500 milhões de dólares aplicada pelo Departamento de Justiça dos Estados Unidos ao Google[10]. A decisão, de 2011, penaliza a empresa por anunciar e possibilitar a venda de remédios canadenses proibidos no país desde 2003 (Zuboff, 2019, p.475). Ignorar a legislação de drogas é apenas uma das facetas dessa indiferença que coloca o lucro em primeiro plano. As empresas já aceitaram anúncios antissemitas[11] em suas plataformas. E todas as vezes em que são criticadas as companhias pedem desculpas[12], como se desconhecessem o funcionamento de seus algoritmos, orientados ao consumo, ignorando princípios éticos e democráticos.

É por isso que a autora enxerga o fenômeno como "parte de uma alarmante tendência global em direção ao que muitos cientistas políticos agora enxergam como um abrandamento das atitudes do público em relação à necessidade e à inviolabilidade da própria democracia" (Zuboff, 2019, p. 482). A que tipo de democracia Zuboff (2019) se refere? A autora deixa transparente que se trata do modelo liberal, baseado em um sistema eleitoral, na representação política e na separação dos poderes executivo, legislativo e judiciário. Sua teoria não explora a incompatibilidade entre a democracia – em que as regras são públicas e iguais para todos – com o próprio capitalismo, em que os interesses privados operam para a reprodução das desigualdades.

---

[10] Google Forfeits $500 Million Generated by Online Ads & Prescription Drug Sales by Canadian Online Pharmacies. Disponível em https://www.justice.gov/opa/pr/google-forfeits-500-million-generated-online-ads-prescription-drug-sales-canadian-online. Acessado em 7/2/19.
[11] Facebook Enabled Advertisers to Reach 'Jew Haters'. Disponível em https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters. Acessado em 7/2/19.
[12] Google pede desculpas por exibir anúncios no YouTube ao lado de vídeos ofensivos. Disponível em https://g1.globo.com/tecnologia/noticia/google-pede-desculpas-por-exibir-anuncios-no-youtube-ao-lado-de-videos-ofensivos.ghtml. Acessado em 7/2/19.

As transformações pelas quais o Google passa no início do milênio são centrais para se compreender como a proteção de dados pessoais e a privacidade se tornam fundamentais nas democracias contemporâneas. E tudo isso ocorre antes de 2005. Não havia Twitter, nem Facebook, muito menos *iPhone*. Ainda estava por vir o pior; a segunda fase do capitalismo de vigilância e o fenômeno da Internet das coisas que exponenciaram o mercado de dados pessoais.

Apenas em 2017, o mercado da Internet das coisas movimentou 35,7 bilhões de dólares. O mesmo estudo estima que, em 2023, o valor chegue à 150.6 bilhões[13]. O capitalismo de vigilância se consolida de forma rápida e silenciosa a partir da experiência individual gratuita. Ou como bem resume o diretor executivo da Apple, Tim Cook; "se o serviço é gratuito, você não é o consumidor, mas o produto[14]". Os dados pessoais transformaram-se em objeto de valor para as empresas de tecnologia, enquanto a maioria das pessoas ignorava, ou não se importava com o que ocorria.

O ano de 2005 representa outro grande salto para a economia de dados a partir do lançamento do Google Maps e a expansão da tecnologia móvel, que Zuboff (2019) caracteriza como a segunda fase do capitalismo de vigilância. Ela pode ser caracterizada por cinco grandes transformações; o acesso móvel à Internet e aos aplicativos, o aumento da capacidade de armazenamento de informações, a coleta e comercialização de dados pessoais, a concentração de conteúdo nas mídias sociais e a automatização promovida por algoritmos inteligentes.

A mudança mais evidente está na transição da computação pessoal para a mobilidade dos celulares e, mais recentemente, os objetos inteligentes da Internet das coisas. No início do milênio, os computadores de mesa e a conexão a cabo eram as principais ferramentas de acesso à web. Nos últimos anos, os dispositivos móveis e a Internet sem fio, aliadas a uma capacidade de armazenamento cada ver maior, deslocaram a forma de acesso. Neste contexto é importante enfatizar que, inicialmente, até havia um mercado competitivo na área de dispositivos móveis, com sistemas como o Windows Phone, *Blackberry* e *Symbian*. Entretanto, nos anos mais recentes observa-se a predominância do sistema Android, pertencente à Alphabet. Segundo a *Statcounter*, em 2018, o Android era responsável por mais de 75% do mercado de sistemas operacionais móveis[15].

Se na década de 1990, havia alguma competitividade entre os sistemas operacionais para computadores de mesa, inclusive a alternativa do software livre, o cenário de 2019 e 2020 não apresenta muitas opções de sistemas operacionais além do Android e do *IOs*, da Apple. Os poucos sistemas operacionais livres para celulares são caracterizados por uma baixa compatibilidade com os

---

[13] Global Smart Homes Market 2018 by Evolving Technology, Projections & Estimations, Business Competitors, Cost Structure, Key Companies and Forecast to 2023. Disponível em <https://www.reuters.com/brandfeatures/venture-capital/article?id=28096>. Acessado em 7/2/19.
[14] Google is collecting data on schoolkids. Disponível em https://mindmatters.ai/2018/09/google-collecting-data-on-schoolkids/. Acessado em 7/2/19.
[15] Statcounter. Dispolnível em < https://gs.statcounter.com/os-market-share/mobile/worldwide >. Acesso em 30/2/19.

hardwares disponíveis no mercado e alta complexidade de instalação e configuração. Com isto ficam restritos a uma pequena comunidade técnica.

Realizadas estas ponderações, é necessário ressaltar ainda que, da mesma forma que os aparelhos de conexão se tornaram menores e mais potentes, aumentou também sua capacidade de armazenamento. Segundo dados da IBM, a humanidade produz 2,5 quintilhões de informações por dia apenas em 2017[16]. O mesmo relatório destaca 90% dos dados existentes no mundo foram produzidos apenas nos últimos dois anos, ou seja, desde 2015. Esta agregação de informações é conhecida pelo termo em inglês *big data*, fenômeno tecnológico que envolve a coleta, quantificação, integração e processamento de informações digitais que registram os aspectos mais triviais do cotidiano (Baruh e Popescu, 2017; Tien, 2013).

Prosseguindo na descrição dos principais fenômenos característicos da segunda fase do capitalismo de vigilância, destaca-se como as mídias sociais foram responsáveis pela concentração do tráfego do conteúdo online criando verdadeiros "jardins murados" (Dantas, 2010). Estas plataformas e seus filtros cerceiam a diversidade criando verdadeiros condomínios, ou espaços privados. A metáfora dos jardins murados é útil para compreender estas transformações. Se a Internet um dia já foi um vasto campo aberto à exploração, com o passar do tempo, grandes corporações adquiriram os principais terrenos disponíveis, centralizaram todo o tráfego passando a controlar o fluxo de informações. As mídias sociais, compreendidas neste contexto tanto como plataformas web, como aplicativos, centralizaram tanto o conteúdo gerado pelas pessoas, como também passam a atuar como *gatekeepers* da informação. Este conceito do jornalismo ilustra como as plataformas – mídias sociais, mecanismo de busca, aplicativos, dentre outros – criam filtros a partir de regras e critérios privados, pouco transparentes para o público.

Longe de esgotar o debate sobre as mídias sociais, que será aprofundado adiante, é importante enfatizar desde já que estes sistemas possibilitam com que cada pessoa seja o curador de seu próprio conteúdo, entretanto dentro dos limites e filtros impostos pelas plataformas. Trata-se do paradoxo da liberdade controlada, ou seja, a capacidade de se expressar de acordo com parâmetros já definidos. Ainda assim, é preciso pontuar desde já, que indicadores de estudos comportamentais, que precedem a Internet, ressaltam que; as pessoas buscam evidências sobre o que já acreditam (viés de confirmação) e se aproximam de outras com pontos de vista semelhantes (homofilia) (Sunstein, 2002). Portanto, quando se discute as câmaras de eco, conhecidas como "bolhas" (Pariser, 2011) é preciso considerar que se trata de um fenômeno social anterior às tecnologias da informação e comunicação.

---

[16] 10 Key Marketing Trends for 2017. Disponível em < https://www-cmswire.simplermedia.com/cw-cp-ibm-2017-03.html?utm_source=cmswire.com&utm_medium=email&utm_campaign=cm&utm_content=wir-170430-0915>. Acessado em 6/10/19.

Ocorre que estes filtros são cada vez mais automatizados pelos algoritmos destas plataformas. A partir dos dados pessoais coletados e tratados por máquinas surgem sugestões de conteúdo, a mídia direcionada, dentre outras experiências mediadas pelas tecnologias. Algoritmos simples, ou inteligentes, analisam, comparam e tratam informações dos mais variados formatos a todo momento.

A principal diferença é que enquanto os algoritmos são códigos computacionais escritos para resolver problemas específicos, algoritmos inteligentes – sejam eles chamados de inteligência artificial ou *machine learning* – são programados para solucionar problemas. O próprio programa assimila a resolução, mas como "eles não aprendem ou raciocinam como os humanos, isso pode fazer com que seus resultados sejam difíceis de prever e explicar" (Tutt, 2017, p. 87). Seus efeitos podem ser simples; um programa fechar sem salvar o trabalho feito, mas podem ser complexos quando suas consequências incidem diretamente na sociedade.

Cada vez mais as pessoas estão submetidas às decisões automáticas dos algoritmos, sem que saibam de que forma foi feita a escolha, ou seleção. Como argumenta O'Neil (2016) a falta de transparência sobre seu funcionamento indica a tendência de que estes mecanismos segregam determinadas informações, privilegiando outras, reproduzindo padrões de preconceito e discriminação de gênero, de raça e de renda, dentre outras, reforçando assim o aprofundamento das desigualdades da sociedade.

Portanto, em pouco mais de dez anos, a ausência da regulação da proteção de dados pessoais nos Estados Unidos possibilitou não apenas a consolidação do Google, como observou o Facebook coletar e vazar dados sem que estas empresas fossem responsabilizadas por sua interferência em processos sociais complexos. Inclusive nas regras e métodos procedimentais dos sistemas eleitorais de democracias consideradas como consolidadas como a inglesa e americana. A atuação da empresa *Cambridge Analytica* na escolha do Reino Unido em sair da União Europeia, e a eleição de Donald Trump, nos Estados Unidos, possuem características semelhantes; as empresas tinham um amplo conhecimento do público, pouco ou nenhum comprometimento com a reciprocidade orgânica com a visão coletivista da sociedade – ou com a própria democracia – e foram marcados por uma indiferença radical para com a ética e a verdade. Exemplos semelhantes localizados na América Latina são o uso de disparos automatizados por *Whatsapp* que marcaram as eleições presidenciais de 2018 no Brasil[17] e o plebiscito sobre o acordo de paz na Colômbia em 2016, em que o voto "em defesa da família" impulsionou a vitória do "não" ao acordo de paz negociado por décadas[18].

Em todos estes exemplos, observa-se a convergência entre recursos e regras, essenciais para

---

[17] WhatsApp confirma: eleições de 2018 tiveram disparo ilegal de mensagens. Disponível em https://www.tecmundo.com.br/software/146595-whatsapp-confirma-eleicoes-2018-tiveram-disparo-ilegal-mensagens.htm. Acesso em 10/12/19.

[18] Voto evangélico é chave na vitória do 'não' no plebiscito da Colômbia. Disponível em https://brasil.elpais.com/brasil/2016/10/12/internacional/1476237985_601462.html. Acesso em 10/12/19.

o exercício da dominação (Bourdieu, 2007). Em outras palavras, as empresas de tecnologia possuíam os recursos, enquanto o governo não realizava nenhum tipo de intervenção, ou regulação. Além opacidade sobre a forma com que os algoritmos destas companhias operam, há uma tentativa constante de impor à sociedade as regras determinadas pelas próprias companhias. É neste sentido que se compreende que o "privado" nunca foi tão político como na atualidade.

Por fim, é fundamental compreender a dimensão coletiva do tratamento das informações pessoais, que impacta toda sociedade, conectada ou não a Internet. O tratamento de dados pessoais transformou-se em "uma forma insidiosa de discriminação entre indivíduos e grupos, com alguns considerados dignos de vários privilégios, como ofertas especiais de produtos de consumo (...) e outros considerados indignos" (Nissembaum, 2009, p.80). Além disso, observa-se a transição da coleta de dados do universo digital para o mundo físico. Se inicialmente o tratamento de dados pessoais focava no indivíduo, mais recentemente os algoritmos inteligentes querem compreender populações e seus comportamentos (Zuboff, 2019). Portanto o debate sobre a proteção de dados pessoais e privacidade é fundamental para as democracias contemporâneas e será aprofundado no segundo capítulo do trabalho. Realizada esta contextualização sobre o papel dos algoritmos na sociedade, prossegue-se para a conceitualização da privacidade a partir da discussão sobre a dicotomia público privada, estruturante das democracias liberais.

1.1 - O público e o privado nas teorias da democracia

Nesta seção serão abordadas as principais referências de teorias da democracia que analisam a divisão entre o público e o privado e suas transformações ao longo dos séculos. Diferentes abordagens enxergam estes espaços de formas diversas, por vezes até de forma antagônica. A discussão está estruturada de um ponto de vista histórico, partindo da antiguidade até a atualidade e os impactos que a web e a Internet têm na esfera pública e privada. Busca-se apresentar a complexidade teórica e histórica da distinção entre o que é público e privado e sua importância para o pensamento liberal, sem deixar de contrapô-lo com outras teorias políticas, em especial o ponto de vista feminista. Em seguida, argumenta-se que, diante das tecnologias da informação e comunicação, os limites entre o que é público e privado se tornam ainda mais híbridos e a metáfora espacial que divide os espaços deixa de ser funcional.

Conclui-se este primeiro capítulo destacando o surgimento do conceito de privacidade e explorando algumas de suas principais dimensões, tais como autonomia, segurança, transparência e liberdade, sem deixar de investigar aspectos subjacentes como a intimidade e classe. Ao debater estes conceitos aprofunda-se ainda em questões como o contratualismo e o neoliberalismo, além das transformações sobre o exercício de direitos e liberdades.

A consolidação da ideia da privacidade individual é relativamente nova no pensamento social, entretanto a concepção de esferas públicas e privadas data da Grécia antiga. A distinção do que é público e do que é privado é culturalmente formada e sensível ao contexto histórico. O que se compreende como público, ou privado, se transforma histórico e culturalmente, mas também de acordo com o discurso que é mobilizado. A distinção, por vezes, é entre o que é político do que não é político, por outras, entre o que é do governo e o que é do mercado, ou até mesmo o que é doméstico, ou não.

De forma que diferentes correntes da teoria da democracia compreendem esta distinção de forma diversa. Por exemplo, "os teóricos liberais muitas vezes contrastam a esfera política (o Estado), a esfera de poder, força e violência, com a sociedade (o domínio privado), que é a esfera do voluntarismo, da liberdade e da regulação espontânea" (Pateman, 2013, p.67). A teoria marxista, por sua vez, explora a crítica à propriedade privada e ao livre mercado. Outras abordagens enfatizam a oposição entre o que é particular e entre o que é universal. Além destes aspectos, a dualidade entre o privado e o público está muitas vezes associada ao território, ou seja, o que está dentro de casa e o que está fora.

Por sua vez, Weintraub (1997) destaca dois critérios em que público e privado se contrastam; "o que está escondido versus o que se encontra aberto, revelado ou acessível" e "o que é individual versus o que é coletivo, ou afeta o interesse de uma coletividade de indivíduos" (p.5). Em outras palavras, o autor adota os parâmetros de publicidade e coletividade para analisar a distinção entre as esferas pública e privada. Como pode-se observar a distinção entre o que é público e o que é privado se torna complexa de acordo com a abordagem mobilizada. Isto ocorre por quê;

> Existem diferentes sentidos de "privado" e de "público" em jogo. "Público" por exemplo pode significar (1) relacionado ao estado, (2) acessível a todos, (3) uma questão comum a todos e (4) pertencente ao bem comum, ou de interesse partilhado. Cada uma destas corresponde a um sentido contrastante de "privado". Somado a isso existem dois outros significados de "privado" pairando na superfície: (5) pertencente a propriedade privada em uma economia de mercado e (6) pertencente a vida pessoal ou doméstica, incluindo a vida sexual. (Fraser, 1992, p. 71)

Em um esforço teórico de análise sobre a teoria e política da divisão entre esferas público e privada Weintraub (1997) oferece quatro grandes formas em que a distinção entre público e privado são apresentadas no pensamento político e social; a abordagem clássica republicana, uma interpretação com foco nos aspectos da sociabilidade da esfera pública, o modelo liberal econômico, e por fim problematizações colocadas pela teoria política feminista (Weintraub, 1997, p.7). Além destas, destacamos também as contribuições marxistas para o debate sobre a separação do público e privado. A seguir explora-se cada uma delas aprofundando as contribuições históricas e

transformações da compreensão do que é público e do que é privado e sua relação com o exercício dos direitos e liberdades.

Na tradição grega, o privado, que se referia à família e a casa, se subordinava ao público, que era a *polis*, local de exercício da cidadania e da política (Saxonhouse, 1983). A *polis* que agregava a comunidade política era o local da prática da *isegoria*, liberdade não apenas de falar, como também de ser escutado, ou seja, o espaço de afirmação entre iguais - os homens não escravos, excluindo assim, mulheres e crianças (Wood, 2003).

De fato, "as primeiras menções sobre o termo privado estão associadas à propriedade privada e são encontradas nos trabalhos de Platão e Aristóteles" (Papacharissi, 2010, p. 27). As terras privadas, que envolviam o domínio da casa dos homens livres estavam presentes na sociedade grega, mas as regras da *polis* impunham limites à propriedade privada e restringiam o direito de herança tal como o conhecemos atualmente (Papacharissi, 2010). De forma que se pode verificar uma distinção entre as esferas, mas não uma separação.

Por sua vez, "o conceito de *res publica*, como oposto de *res privatae*, foi uma invenção dos Romanos" (Saxonhouse, 1983, p.363). Na antiga Roma, a *civitas*, que corresponderia à *polis* grega, era o espaço de convivência social, da cidadania regida por leis. No direito romano a noção da coisa pública estava relacionada ao pertencimento a república, enquanto o *privatus* se referia ao cidadão, que não fosse um magistrado, ou membro do exército, pois estes eram parte da república romana. Sobretudo;

> "Privado" em oposição a "público" é um dos adjetivos mais empregados da língua latina, porém não delimita positivamente a vida privada; seu sentido é negativo: qualifica o que um indivíduo pode fazer sem atentar contra seus deveres e suas atitudes de homem revestido de uma função pública. (Duby e Ariès, 2009, p. 151)

Em outras palavras, o foco da vida social estava naquilo que era público. Na antiga Roma, as latrinas eram coletivas e "todo mundo tinha acesso aos espetáculos e aos banhos, inclusive os estrangeiros; vinha gente de longe para ver os gladiadores em uma cidade. A melhor parte da vida privada transcorria em estabelecimentos públicos" (Duby e Ariès, 2009, p. 179). A própria prática do evergetismo, que consiste em presentes luxuosos para a comunidade, por parte da elite política romana, confunde a função do homem público do privado, já que eles financiavam as obras e monumentos públicos.

Nas sociedades grega e romana a ênfase estava no espaço público, nos assuntos de interesse comum e a liberdade e a autonomia eram exercidas (pelos homens) em locais abertos. Uma importante contribuição de Weintraub (1997) ocorre quando o autor destaca o surgimento da ideia de soberania durante o império romano, descrevendo-a como "um aparato centralizado, onipotente e unificado que rege acima da sociedade e que governa por meio do cumprimento das leis" (p. 11). Mesmo com a

presença de uma estrutura de estado, ou de soberano que governe, o pensamento clássico tem foco na cidadania, ou seja, no sujeito capaz tanto de fazer as normas e regras, como de ser governado. Nesta tradição "a esfera apropriada para a dominação é do espaço privado da casa, estruturada em relações 'naturais' de desigualdade; entre senhor e escravo, pai e crianças, marido e mulher" (Weintraub, 1997, p.12). O cidadão livre é aquele que participa na resolução de temas públicos e participa do processo de decisão da comunidade política. Entretanto, com o declínio do império romano e a conformação dos feudos na Europa antiga, a participação política e o exercício da cidadania se transformam.

Weintraub (1997) sublinha que, tanto a noção de cidadania, como a de soberania, desapareceram durante a idade média, assim como a valorização do domínio da coletividade (*res publica*), que perderia espaço público encolhendo no pátio das novas habitações. É neste período que todo o estilo arquitetônico, que privilegiava espaços comuns, se transforma. Surgem os cômodos individualizados, como os quartos (Duby e Ariès, 2009). De fato, "a linha entre a esfera privada e a esfera pública passa pelo meio da casa. As pessoas privadas saem da intimidade de seus quartos de dormir para a publicidade do salão; mas uma está estreitamente ligada a outra" (Habermas, 1984, p.61). Se até no ambiente doméstico dos séculos XVII e XVII as esferas se entrelaçam, pode-se observar que o processo de individualização, em termos arquitetônicos iniciado com os quartos, é uma complexa transformação cultural. É nessa mesma época que eclodem o fenômeno das cartas e dos diários pessoais, em especial dentre a aristocracia europeia (Duby e Ariès, 2009; Habermas, 1984). Durante a idade média observa-se também o surgimento do isolamento como forma de reflexão, em especial a partir dos monges da igreja católica, que se retiravam do convívio social. É neste sentido que a palavra latina de *privatio* era utilizada no período significando "afastar-se" do convívio social (Duby e Ariès, 2009). Manifesta-se, assim, o delineamento da noção de intimidade.

Para Weintraub (1997) este período histórico do antigo regime não foca no Estado, na cidadania, ou vida privada, e sim na sociabilidade e na domesticidade. Nesta abordagem o público não está relacionado com o governo, ou em assuntos de interesse comum, "a chave não é a solidariedade, ou a obrigação e sim a sociabilidade" (Weintraub, 1997, p. 18). De forma semelhante, Ariés (2009) narra a decadência dos regimes medievais e emergência da família moderna, transformando drasticamente as esferas do que é público e privado, ao agregar novos elementos à vida privada, como a intimidade. O núcleo familiar que se constitui faz com que a sociedade civil, ou seja, tudo que é externo ao que é doméstico, se torne o novo espaço público. O encolhimento do espaço público faz com que o ambiente doméstico seja valorizado enquanto espaço da construção da subjetividade, que antes era exercida nas ruas, em público.

Ao descrever práticas da sociedade do século XVII, Foucault (1988) retrata-as desta forma; "gestos diretos, discursos sem vergonha, transgressões visíveis, anatomias mostradas e facilmente misturadas, crianças astutas vagando, sem incômodo nem escândalo, entre os risos dos adultos; os

corpos *pavoneavam*" (p.9). Em outras palavras, não havia a noção contemporânea de obscenidade, cujas leis vieram a surgir apenas no início do século XIX, quando a separação das esferas instaura as concepções de decência e indecência. A sexualidade ainda não estava confinada "ao quarto dos pais", não havia "mudado para dentro de casa", não havia sido confiscada pela "família conjugal" (Foucault, 1988, p. 10). O autor relaciona a repressão sexual com o próprio surgimento do capitalismo, indicando que "se o sexo é reprimido com tanto rigor é por ser incompatível com uma colocação no trabalho (...) na época em que se explora sistematicamente a força de trabalho, poder-se-ia tolerar que ela fosse dissipar-se nos prazeres" (Foucault, 1988, p. 11). Essas transformações não representam o triunfo do individualismo e sim do núcleo familiar, alterando toda uma gama de relações privadas (Ariès, 1960; Weintraub, 1997). A consolidação de um espaço de intimidade também muda a forma com que as pessoas se sociabilizam em ambientes não domésticos.

É neste contexto que Habermas (1984) descreve a emergência da família burguesa, em contraposição a uma aristocracia, que já era reconhecida e tinha acesso aos bens culturais. A "emancipação político econômica" da burguesia "é concretizada na participação no comércio e nas trocas" (Habermas, 1984, p. 63), ou seja, a ascensão do mercantilismo, acompanhado por um crescente acesso aos bens culturais, antes exclusividade da aristocracia.

Em termos arquitetônicos e políticos isso significa a conformação das cidades modernas, com limpeza urbana, comércio, transportes e espaços públicos. Para Habermas (1984) estas cidades se caracterizam como "uma primeira esfera pública literária, que encontra as suas instituições nos *coffee houses*, nos *salons* e nas comunidades de comensais" (p.45). Em contraposição, Weintraub (1997) enfatiza que se trata de um "espaço de coexistência heterogênea, não de solidariedade inclusiva ou de ações coletivas conscientes (...) não é um espaço (...) de debate para alcançar um consenso racional para encaminhar questões comuns" (p.25). Esta é a diferença com relação ao modelo clássico de cidade; o espaço público não é mais o local do exercício das liberdades e direitos políticos. Portanto, antes de prosseguir, dedica-se alguns parágrafos para debater o conceito de esfera pública de Habermas (1984), que é central para teorias da comunicação e das ciências sociais.

Na obra em que cunhou o conceito, Habermas (1984) inicia analisando a formação da burguesia e da esfera pública, bem como a divisão entre a vida privada e o Estado, destacando o mercado como esfera emergente. Para o autor, a esfera pública literária, vivenciada nos cafés e na vida cultural da burguesia europeia dos séculos XVII e XVIII, evolui para uma esfera pública política, consequência da "emancipação política da sociedade civil burguesa em relação à regulamentação mercantilista, sobretudo em relação ao regime absolutista" (Habermas, 1984 p. 74). A independência da classe burguesa se consolida no associativismo, na livre iniciativa e na conformação de uma opinião pública que passa não apenas a criticar o Estado absolutista, como também a formular demandas. É "a ideia de uma esfera pública enquanto um corpo de pessoas privadas reunidas para

discutir questões de interesse público e comum" (Fraser, 1992, p. 58). O autor é categórico ao afirmar que "uma esfera pública funcionando politicamente aparece primeiro na Inglaterra na virada do século XVIII" (Habermas, 1984, p.75). Ocorre que em seguida, ele diagnostica a decadência da esfera pública burguesa a partir da transformação dos cidadãos em consumidores e da influência dos meios de comunicação de massa, que reorganizam a vida social. Para o autor, se inicialmente a separação entre sociedade civil e estado era benéfica, no sentido de gerar críticas e demandas para um bem-estar social, a opinião pública, na era dos meios de comunicação de massa, serve para legitimar a atuação do Estado.

A primeira parte da obra de Habermas (1984) descreve um período histórico em que se observa a retomada da noção de cidadania e de soberania, a partir da formulação da ideia de sociedade civil, de uma era das sociedades, ou até mesmo uma nova organização das relações sociais. Weintraub (1997) destaca "a concepção de Tocqueville de 'sociedade política', a concepção de Hannah Arendt de 'domínio público' e a concepção de Habermas de 'esfera pública' como representantes de alguns dos esforços mais significantes de caracterizar e teorizar esta esfera da vida social" (p.15). Ainda assim, o autor critica as três abordagens dado que todas elas estão ancoradas na oposição entre o que público e o que é privado, argumentando que "a esfera pública (e a política) não pode ser reduzida ao Estado, a esfera da vida social fora do Estado (e de seu controle) não pode ser identificada como privada" (Weintraub, 1997, p.15). Esta nova sociedade civil tem interesses e influência no Estado, justamente por isso não são esferas desconectadas. Além disso, esta esfera pública pressupõe que os racionais debates ocorram entre iguais, ignorando as assimetrias e desigualdades de classe, raça e gênero.

Muitas críticas foram realizadas à obra de Habermas (1984). Dentre elas destaca-se aquelas provenientes da teoria política feminista. Fraser (1992) enfatiza que "o problema é que Habermas não apenas idealiza a esfera pública liberal como também falha em examinar outras, não liberais, não burguesas, esferas públicas concorrentes" (p.61). Trata-se do conceito de "contra públicos", que a autora desenvolve para explicar que há diversidade na esfera pública para além do discurso hegemônico. Para ela os contra públicos "contestam as normas excludentes do público burguês, elaborando estilos alternativos de comportamento político e normas alternativas do discurso público" (Fraser, 1992, p. 116). O conceito é importante pois enfatiza que não existe o consenso na esfera pública. Seu espaço está em constante disputa, ainda que "a esfera pública oficial seja a fonte institucional primária da construção do consenso, que define um novo modo hegemônico de dominação" (Fraser, 1992, p. 117). Os meios de comunicação de massa, portanto, operam para legitimar os discursos da classe dominante. Diferentemente de Habermas (1984) que critica a mídia com relação ao Estado.

Ao identificar os contra públicos, Fraser (1992) reconhece que esta dominação enfrenta estratégias de resistência, muitas vezes "invisíveis" e decisões "contraditórias" (Scott, 1990; Sunstein, 2009). De fato, o discurso público é diferente daquele realizado de forma íntima. Por trás de uma aparente conformidade e obediência, os sujeitos realizam constantemente atividades de insubordinação com relação ao poder instituído (Scott, 1990).

Em 1990, em um prefácio à nova edição de "Mudança estrutural da esfera pública", Habermas (2014) responde parte das críticas realizadas a seu trabalho, ainda que admita que "continuo pensando que esse tipo de esfera púbica forma o plano de fundo histórico para as formas modernas de comunicação pública" (Habermas, 2014, p. 43). Por um lado, o autor reconhece a existência de uma esfera pública hegemônica. Ainda assim, insiste na existência de uma esfera pública política "em que se cruzam dois processos; de um lado a criação comunicativa do poder legítimo; de outro o uso manipulador dos meios de comunicação de massa para produzir a lealdade das massas" (Habermas, 2014, p. 80). De fato, é inquestionável toda a crítica da Escola de Frankfurt aos meios de comunicação de massa e os processos midiáticos desencadeados a partir de sua proliferação. Por outro lado, a abstração de uma esfera pública política, em que processos comunicativos levam a deliberação racional de questões de interesse comum, se mostrou pouco eficaz. Realizadas estas ponderações com relação ao conceito de esfera pública, que será retomado adiante com a proliferação da Internet, prossegue-se para a análise do modelo liberal de distinção das esferas público e privado, cuja visão hegemônica impera nas democracias ocidentais contemporâneas.

O modelo liberal econômico deve ser enxergado tendo em mente as transformações históricas ocorridas a partir da reforma protestante, do crescimento do pensamento republicano e da expansão da comunidade político e cultural ocorrida a partir dos séculos XVII e XVIII na Europa. A separação entre o que é público e o que é privado nas sociedades contemporâneas é um princípio fundador do liberalismo. Nesta visão hegemônica, a separação se encontra ancorada na divisão entre os assuntos que são de interesse comum, ou seja, que necessitam da interferência do Estado e os assuntos que são de interesse privado, nos quais os governos não ditam as regras e sim as leis e o mercado. Para o pensamento liberal a dicotomia entre o público e privado está relacionada ao que é assunto governamental, ou individual, sendo que os direitos individuais de liberdade e autonomia devem prevalecer. Está na base desta corrente a ideia do indivíduo enquanto unidade política e, apesar de haver o reconhecimento da família enquanto entidade de direitos, a autoridade no âmbito privado é dos homens.

Esta tradição, fundada no contrato social, cria uma divisão entre o que é público e o que é privado e parte da premissa de que a regulação das relações privadas seria uma intrusão do Estado nos direitos individuais. Se durante a idade média a sociabilidade estava calcada na família, com o liberalismo, observa-se o início de um processo de individualização a partir da valorização desses

direitos individuais masculinos. De fato, “uma esfera privada que funciona como a base da emancipação cívica está em harmonia com os valores do individualismo, autonomia, auto expressão que são prevalecentes nas sociedades modernas” (Papacharissi, 2010, p.134). De forma que a origem do liberalismo e do capitalismo está ancorada em uma negligência da esfera privada, pois “precisamente porque o liberalismo conceitua sociedade civil de forma abstrata em relação à vida definida como doméstica, esta continua a ser “esquecida” na discussão teórica” (Pateman, 2013, p. 59). Esta corrente teórica defende que cada indivíduo é livre para efetuar suas escolhas, e que os contratos são a base de uma sociedade em que as partes, de forma privada, podem negociar sem a necessidade de interferência do Estado. Portanto, o pensamento liberal contemporâneo cultiva “a suposição de que os setores público e privado não são compatíveis” (Papacharissi, 2010, p.31). O pano de fundo destes debates está na resposta a duas clássicas abordagens sobre a ordem social; como organizar os conflitos sociais e harmonizar interesses particulares em uma dada sociedade.

São reconhecidas diferentes perspectivas clássicas que respondem a estas questões (Weintraub, 1997; Papacharissi, 2010). De um lado John Locke e Adam Smith apostando que a harmonização dos interesses particulares ocorre a partir da livre iniciativa e do mercado. De outro lado, o pensamento de Hobbes e Bentham, que enxergam a necessidade de um agenciamento coercitivo acima da sociedade para seu bom funcionamento, ou seja, o Estado. O argumento de Hobbes (1987) é de que no estado de natureza impera o conflito e a violência entre indivíduos. Para ele a ausência de hierarquia é um problema social resolvido a partir do contrato, em que as pessoas renunciam a sua soberania e liberdade, em troca da segurança de não sofrerem as brutalidades presentes no estado de natureza. De forma simplificada, enquanto Locke e Smith apostam na esfera privada para a solução do conflito de interesses das sociedades, Hobbes e Bentham apresentam a necessidade da imposição de limites pelo Estado.

A última abordagem que Weintraub (1997) propõe para debater a questão da divisão entre público e privado é a teoria política feminista. Antes de prosseguir, é importante pontuar que esta teoria, nas suas mais variadas vertentes, que vão de visões mais radicais a postulações liberais, se apresenta, em geral, como um contraponto ao pensamento hegemônico das ciências sociais. Isto ocorre devido ao fato de historicamente a teoria social foi pensada a partir de uma perspectiva masculina, branca, burguesa, universal e abstrata, ou seja, como se todas as pessoas estivessem nas mesmas condições estruturais e não existissem diferenças de classe, gênero, raça, dentre outras (Pateman, 1993; Walby,1990; Delphy, 1980; Phillips, 2011; Okin, 2008). Em face ao surgimento dessa literatura, alguns teóricos contemporâneos, reconheceram “que a exclusão das mulheres foi também constitutiva para a esfera pública política, (...) determinada também em termos de gênero em sua estrutura e sua relação com a esfera privada” (Habermas, 2014, p.46). Excluídas da esfera política, até pelo menos a adoção do sufrágio universal, diferentes vertentes do feminismo “enfatizaram que

as forma com que a divisão entre público e privado estava relacionado ao gênero, tanto em termos de estrutura social, como de ideologia" (Weintraub, 1997, p. 28). A exclusão da esfera privada da política contribuiu para a manutenção de relações de dominação e autoridade masculinas, que interferiram sistematicamente na autonomia feminina.

Neste sentido, uma das principais contribuições de debate feminista é destacar que o que se passa na esfera privada influencia a esfera pública, portanto "os domínios da vida doméstica (pessoal) e da vida não-doméstica (pública) não podem ser interpretados isoladamente" (Okin, 2008, p. 305). O que ocorre na esfera privada não pode ser excluído de regras de justiça, igualdade e cidadania. Esta separação entre as esferas, entre o que seria universal, e o que seria particular, é baseada em uma narrativa de conflito, fundamentada em uma lógica dialética e binária, portanto, não dá conta do caráter relacional entre o que é público e o que é privado.

A sociedade civil, conformada a partir do pensamento liberal, exclui as mulheres e crianças de sua sociedade política. Historicamente, a separação entre as esferas serviu para perpetuação da dominação masculina e a domesticação das mulheres (Pateman, 1993). Nas democracias liberais, por muito tempo, imperou o consenso de que o Estado não deveria interferir no âmbito privado. Pateman (1993) descreve como o contrato sexual é o pano de fundo que sustenta as democracias liberais, ao colocar as mulheres submissas na esfera privada. Todo o trabalho doméstico desempenhado pelas mulheres é o que sustenta o indivíduo liberal na sociedade moderna, ainda assim, o espaço privado não é compreendido como parte do que é político, tampouco do que é produtivo (Delphy, 1980). Como bem pontua Weintraub, (1997), na tradição clássica "o ambiente doméstico compreendia tanto a família quando a vida econômica, dado que o ambiente familiar era a principal instituição reguladora da produção e distribuição" (p.32). No pensamento liberal, que não leva em consideração a esfera privada, todo o trabalho doméstico realizado, tal como o cuidado com as crianças e idosos e a preparação de alimentos, por exemplo, não é tratada como um trabalho produtivo. Delphy (1980) argumenta que "não há diferença entre os serviços domésticos realizados pelas mulheres e os outros bens e serviços ditos produtivos, realizados e consumidos na família" (p. 105). Ela demonstra como nas famílias rurais, que são produtoras e consumidoras ao mesmo tempo, não existe diferença entre produção e consumo, como nas sociedades capitalistas. Ao negligenciar a esfera doméstica, todo o trabalho exercido neste ambiente se torna também desvalorizado, entretanto no ambiente externo este trabalho "invisível" tem seu custo. De modo que a exclusão da economia da esfera privada no pensamento liberal e no capitalismo contribui também para reforçar a distinção entre público e privado. Portanto, a própria a constituição da família, debatida em parágrafos anteriores, serviu para a emancipação masculina na esfera pública, ao mesmo tempo em que subordinou as mulheres ao espaço privado, de intimidade e de cuidado.

Por fim, Weintraub (1997) destaca pelo menos três grandes contribuições da teoria política

feminista para o debate sobre a divisão entre público e privado:

> Primeiramente, as orientações conceituais de boa parte da teoria política e social ignoraram a esfera doméstica ou trataram-na como trivial. A segunda é que a distinção público / privado em si é muitas vezes tem implicações de gênero e de maneiras quase uniformemente inviáveis. Muitas vezes, desempenha um papel em ideologias que pretendem atribuir aos homens e às mulheres a diferentes esferas da vida social com base em suas características "naturais" e, portanto, limitar as mulheres a posições de inferioridade. A terceira é que, ao classificar instituições como a família como "privadas" - mesmo quando isso é feito de forma ostensivamente neutra em termos de gênero - a distinção público / privado serve frequentemente para proteger abusos e dominação nessas relações e evitar o escrutínio político ou reparação legal (p.29).

Conforme observou-se, os conceitos de público e privado têm seu significado alterado de acordo com a literatura mobilizada, ainda que sua distinção oriente a vida em sociedade. Antes de prosseguir, é preciso ressaltar que a abordagem sobre os conceitos de público e privado apresentada reflete uma visão eurocêntrica, que prevalece em geral nas ciências sociais. Certamente estes conceitos em sociedades compreendidas como “primitivas”, como os indígenas, ou os aborígenes, possuem um sentido completamente diverso.

Destacadas as principais abordagens das ciências sociais com relação à distinção entre público e privado, debate-se a seguir como estas esferas se misturam no ambiente virtual da web. Em primeiro lugar, é necessário ressaltar que “as pesquisas acadêmicas sobre a Internet como uma esfera pública apontam para a conclusão de que as tecnologias digitais online criam um espaço público, mas não necessariamente possibilitam a conformação de uma esfera pública” (Papacharissi, 2010, p. 236). Conforme discutido, boa parte da literatura sobre democracia digital enfatiza as possibilidades deliberativas e de participação deste meio de comunicação, o que levou ao conceito de esfera pública interconectada (Benkler, 2008). Entretanto, ainda que a web tenha impulsionado novas ações políticas e, sobretudo novas formas de expressão e interação social seu caráter essencialmente comercial impede que ela seja considerada como uma esfera pública.

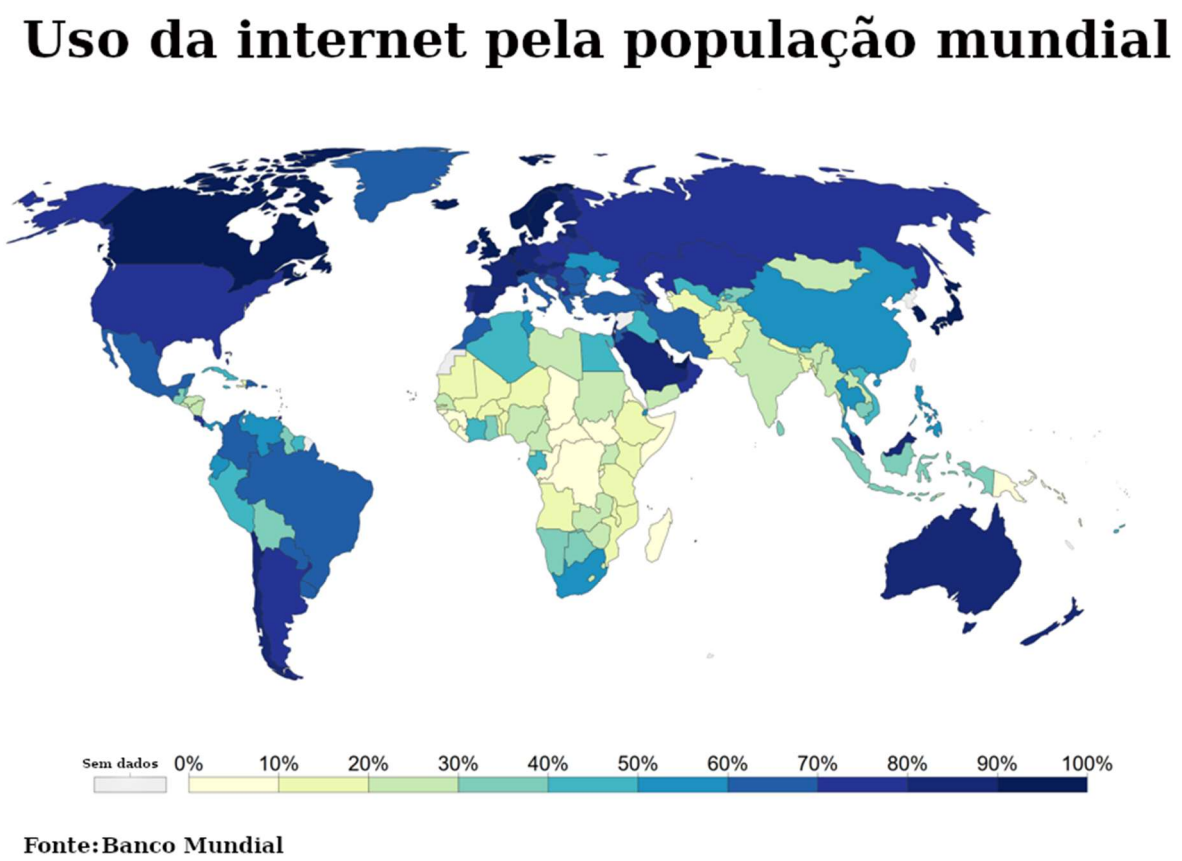
O fato é que quando se introduz o elemento das tecnologias da informação e comunicação, em especial a web, as fronteiras entre o que é público e o que é privado se tornam ainda mais tênues. Isto ocorre porque o fator territorial se dissolve, dado que a partir da web cada pessoa pode estar na esfera privada de sua casa e, ao mesmo tempo, falar para um público amplo e desconhecido. Além disso, os discursos realizados a partir dos espaços “privados” têm o potencial alargado, ou seja, uma vez registrado na Internet, pode ser resgatado a qualquer momento e em outros contextos. Isso faz com que as comunicações privadas estejam sujeitas à exposição pública. Em resumo;

> As tecnologias online prosperam em colapsar as barreiras entre público e privado ao possibilitar oportunidades de expressão que, ao mesmo tempo empoderam e comprometem indivíduos. Sobretudo, a natureza convergente da mídia online cria uma confluência entre os

> domínios social, político, econômico e cultural o que leva a expressões que misturam e emprestam de todas estas esferas de atividade. (Papacharissi, 2015, p. 94).

Esta convergência dos campos da vida social em uma esfera virtual influencia cada vez mais a própria política e o sistema democrático. Isto ocorre porque antes da Internet "o cidadão era ativado por meio da esfera pública, na democracia contemporânea, o cidadão atua politicamente a partir de uma esfera privada de reflexão, expressão e comportamento" (Papacharissi, 2010, p.244). As tecnologias da informação e comunicação possibilitaram a expressão da opinião, a participação política e a interação a partir da esfera privada, em um ambiente que é ao mesmo tempo público, no sentido de ser acessível e visível para metade da população mundial, e ao mesmo privatizado, por ser propriedade de grandes empresas de tecnologia. Ainda que este acesso seja concentrado no norte global e assimétrico com relação a outros países do mundo, conforme observa-se na figura 1.

Figura 1: Uso da Internet pelo mundo.[19]



Papacharissi (2015) argumenta que as pessoas que utilizam as mídias sociais, que se expressam politicamente na Internet, são um "público afetivo". Para ela, a expressão política na

[19] The rise of social media. Disponível em https://ourworldindata.org/rise-of-social-media. Acesso em 2/2/20.

Internet, ao contrário de debates racionais e argumentos impessoais, universais e abstratos, possui um componente emotivo que é balizador das manifestações.

Para embasar seu argumento, a autora realizou um estudo analítico e quantitativo de importantes fenômenos que utilizaram as ferramentas da web para se organizar e dar publicidade a seus atos; o *Occupy Wall Street*, a Primavera Árabe e o movimento dos Indignados na Espanha. De forma resumida, o primeiro deles ocorreu em Nova Iorque nos Estados Unidos e foi deflagrado em 17 de setembro de 2011, como um protesto pela desigualdade econômica e social, mas também pela influência do setor financeiro nas políticas públicas. A Primavera Árabe, por sua vez, ocorreu a partir de 18 de dezembro de 2010, em países como a Tunísia e Egito motivados também pela desigualdade, mas também pela forte repressão das ditaduras de seus países. Já o movimento dos indignados teve início em 15 de maio de 2011, na Espanha, com críticas à classe política e às práticas econômicas adotadas pelo governo.

Estes três eventos tornaram-se objeto de estudo, de forma individual ou conjunta, de diversos autores e consolidaram o fato de que a Internet possibilita novas formas de organização política e de manifestação de opinião. Parte dessa literatura saudou estes eventos como a realização de um novo tipo de organização política, operado por meio da Internet, que promovia o engajamento e a participação (Castañeda, 2012; Milner, 2013). Não se questiona o mérito destes eventos, apenas pondera-se que são fenômenos anteriores às revelações de Edward Snowden sobre as operações de vigilância em massa realizadas pela Agência Nacional de Segurança dos Estados Unidos, em 2013. A divulgação da informação de que todas atividades na web, além de registradas, são monitoradas reforça a tendência da autocensura e, consequentemente da limitação da liberdade de expressão, temas retomados adiante.

A contribuição de Papacharissi (2015), que realizou sua análise a partir de dados do Twitter, é reforçar características das formas de expressão online. Para tanto, ela recorre à três conceitos chave; público em rede, *gatekeepers* em rede e enquadramento em rede (*networked publics, networked framing* e *networked gatekeeping*), cunhados por Barzilai-Nahon (2009). Estes conceitos, tradicionalmente utilizados no jornalismo, se referem ao enquadramento noticioso, ou seja, a abordagem sobre os fatos que expõe mais alguns detalhes enquanto oculta outros. Por sua vez, o processo de gatekeeping refere-se à edição jornalística, o filtro das notícias, ou seja, a seleção do que será noticiado de acordo com a linha editorial, ou outros critérios (Wolf, 2005). Estas funções, exercidas nos meios de comunicação de massa por profissionais dedicados, na Internet são realizadas de forma coletiva, ou seja, "explica como pessoas interconectadas trabalham de forma colaborativa e co-criam narrativas" (Papacharissi, 2015, p. 165). Ainda que a autora foque em fenômenos que mobilizaram multidões nas ruas, é possível observar que as funções de enquadramento, de filtragem e de agendamento se modificam a partir da introdução da web no ecossistema de mídia. Este público

em rede cada vez mais influencia os meios de comunicação de massa tradicionais[20].

A transformação não se dá apenas pela introdução de novas ferramentas, mas também pela centralidade da expressão individual nestes processos, caracterizados como uma forma de performance, que "permitem com que os indivíduos cruzem do particular para público, mas também, potencialmente, do pessoal ao político, ou do individual ao coletivo" (Papacharissi, 2015, p. 98). Para a autora, a forma de expressão em mídias digitais tem uma natureza calcada na "personalização, ou seja, a capacidade de organizar informações com base em uma ordem subjetiva de importância determinada pelos sujeitos" (Papacharissi, 2010, p.237). Ou seja, são "narrativas geradas de forma privada e publicadas em espaços comerciais públicos" (Papacharissi, 2010, p.237). Portanto, as plataformas de conteúdo se tornam os intermediários, os verdadeiros *gatekeepers* contemporâneos, um controle privado sobre o que é apresentado ao público online.

Essa expressão performática online ainda tem um aspecto de brincadeira, de jogo e muitas vezes até de humor. Tal fato pode ser observado no fenômeno dos *memes*, quando uma informação – um vídeo, um GIF animado, uma fotomontagem - é compartilhada muitas vezes em episódios conhecidos como "viralização". Sobretudo "é importante notar que a brincadeira prepara a transição do privado para o público" (Papacharissi, 2015, p.107), ao deixar as pessoas mais confortáveis em se expressar. Por meio do humor, da sátira e da ironia, os *memes* podem ser simplesmente algo irrelevante, como também podem conter críticas a personalidades e políticos.

Além disso, o fato dessa auto expressão na web ser realizada do conforto da tela privada faz com que as pessoas tenham menor pudor em realizar declarações que não fariam em situações face a face. Ademais, a instantaneidade do ambiente virtual facilita que a mobilização potencialize uma espontaneidade com menos filtros, ou autocensura. A intensidade é outro fator notado nesse público afetivo, cujo engajamento pode ser observado não apenas no compartilhamento de *memes*, mas também em gestos de solidariedade e aliança. Um exemplo disso foi a reprodução da hashtag #metoo a partir de outubro de 2017 para a denunciar a prática de assédio sexual em especial no ambiente de trabalho.[21]

Outra tendência que a autora identifica são "ações subversivas articuladas discursivamente

---

[20] No Brasil, exemplos disso são os afastamentos do ator José Mayer, após denúncia de assédio sexual, e do jornalista William Waack, depois que um vídeo com comentários racistas foi divulgado, ambos da rede Globo. Estes acontecimentos reforçam o poder de compartilhamento na Internet. Se no *Occupy Wall Street* o engajamento se deu com a expressão #We Are 99% (nós somos os 99%) no caso do ator global a expressão foi "Mexeu com uma mexeu com todas", ou "agora é que são elas". Estas práticas também se caracterizam por empatia e solidariedade, que é manifestada quase que de forma instantânea por meio dos compartilhamentos. Em ambos os casos se observa novos circuitos de agendamento que forçam os meios de comunicação tradicionais a tratar de temas que o público debate, mas que caso contrário não teriam "valor-notícia".

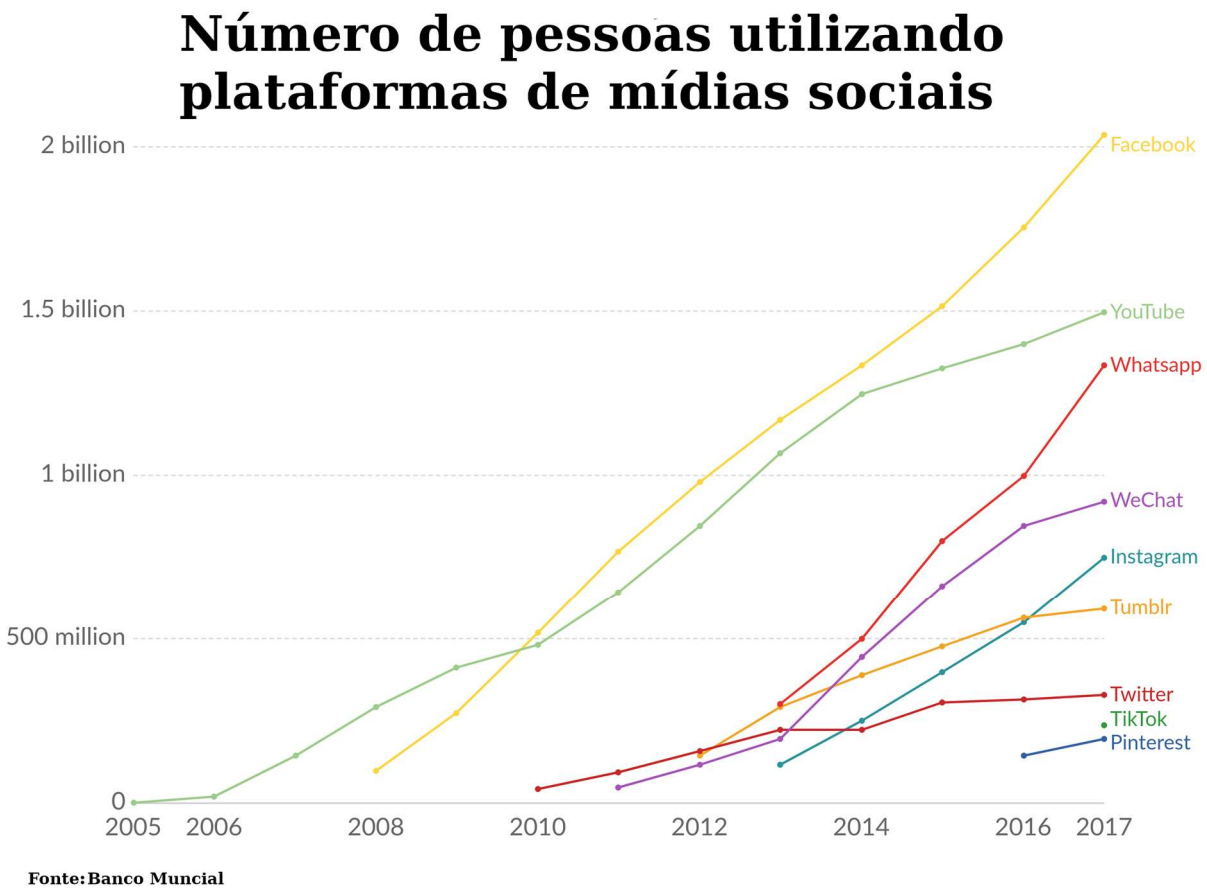
[21] #MeToo: how a hashtag became a rallying cry against sexual harassment. Disponível em < https://www.theguardian.com/world/2017/oct/20/women-worldwide-use-hashtag-metoo-against-sexual-harassment >. Acessado em 25/01/18.

que enfatizam a pluralidade e o agonismo" (Papacharissi, 2010, p.244). Interessante ressaltar que a autora utiliza duas importantes referências para descrever as características da expressão online. Primeiramente o modelo do pluralismo agonístico de democracia (Mouffe, 2005) que reconhece o caráter conflitivo da política e se propõe a reconhecer as disputas entre os atores políticos, mas busca tratá-los como adversários e não inimigos. A outra referência destacada pela autora são os contra públicos (Fraser, 1992) que, por meio da Internet, conseguem ampliar suas formas de expressão.

Em resumo, para a autora, as formas de expressão online se caracterizam pela personalização, pelo antagonismo e pluralidade, pela intensidade e volume. Além disso incorporam funções do jornalismo colocando-as em rede; o enquadramento, o agendamento e o *gatekeeping* são realizados colaborativamente, articulados em rede (Papacharissi, 2015). Ocorre que boa parte do discurso político da web se dá em ambientes que não foram designados para esta finalidade (Wojcieszak e Mutz, 2009). Portanto, pode-se dizer que "o paradoxo da experiência online é que ela oferece às pessoas a possibilidade de se comunicar e interagir com outras na privacidade de suas casas, ao mesmo tempo em que às expõe ao monitoramento e rastreamento sem precedentes" (Nissenbaum, 2009, p.27). Ou seja, ao mesmo tempo em que a web potencializa novas formas de expressão, de organização política e social, sua característica essencialmente cibernética – de registro e controle – reforça a instauração de sistemas de vigilância complexos e retroalimentáveis.

Independentemente do monitoramento das experiências privadas de forma automatizada realizado na web, as mídias sociais ainda são a principal forma de expressão online. Dados do Banco Mundial indicam que mais de cinco bilhões de pessoas utilizam mídias sociais, distribuídas conforme ilustra o gráfico 1.

Gráfico 1: O uso de mídias sociais[22].



Conforme pode-se observar, o Facebook é líder neste mercado, inclusive por ter adquirido as plataformas de conteúdo do *Whatsapp* e Instagram. Ainda assim, merece destaque o crescimento dos chineses com o *TikTok* e o *WeChat*, sendo que este último é um dos pioneiros em implementar métodos de pagamento por meio das mídias sociais.

Realizadas estas considerações, este debate leva à conclusão de que a Internet, ao confundir a distinção entre público e privado, enfatiza que esta dicotomia não reflete a realidade, que é mais complexa e contextual. O que a Internet provoca é um novo conjunto de práticas sociais, que não se adapta facilmente à epistemologia liberal, que organiza nossa compreensão do público e do privado. As tecnologias da informação e comunicação portanto evidenciam que as esferas público e privadas precisam, cada vez mais, estarem desvinculadas de sua metáfora espacial.

A dicotomia entre público e privado se transforma ao longo dos séculos e de acordo com o contexto cultural. Entretanto, a noção de privacidade é recente no pensamento social. A seguir,

[22] The rise of social media. Disponível em https://ourworldindata.org/rise-of-social-media. Acesso em 2/2/20.

trabalha-se com o surgimento deste conceito, algumas de suas dimensões e suas relações com as teorias da democracia.

1. 2 – O conceito de privacidade e suas dimensões

O conceito moderno de privacidade surge como uma reação aos meios de comunicação de massa e a conformação da esfera pública, como narrada por Habermas (1984). O clássico artigo de Warren e Brandeis, de 1890, intitulado "*O direito à privacidade"* é uma crítica à imprensa e uma defesa do direito de ser deixado em paz. Ele é escrito durante a explosão do jornalismo, quando a imprensa perdia seu caráter majoritariamente partidário, passando ao modelo industrial.

Os autores defendem que "a lei existente proporciona um princípio que pode ser invocado para proteger a privacidade do indivíduo da invasão da imprensa, do fotógrafo, ou qualquer possuidor de qualquer outro tipo de dispositivo moderno de gravação e reprodução de cenas, ou sons" (Warren e Brandeis, 1890). A afirmação pode ser atualizada para a crítica aos *paparazzi* e toda imprensa voltada para a vida de celebridades, além dos registros audiovisuais realizados sem autorização prévia, ou consentimento das pessoas. Exemplos atuais são as câmeras de vigilância, fotos em eventos e em locais públicos.

Sendo assim, esta primeira noção de privacidade está relacionada ao direito de ser deixado em paz, que se aproxima do conceito de liberdade negativa (Berlin, 1959), ou seja, a não interferência do Estado, ou no caso, da imprensa. Na tradição liberal a liberdade individual é calcada na esfera privada, entendida como o espaço de autonomia, noção que se contrapõe às perspectivas clássicas, em que a liberdade era exercida no ambiente público (Saxonhouse, 1983). É justamente no contexto de consolidação de um modelo representativo e liberal de democracia que o conceito de privacidade surge.

A partir da conformação do capitalismo, do pensamento liberal e das democracias representativas, observa-se o início de um processo de individualização focado na figura do homem livre, em que as escolhas individuais ganham força e relevância. É justamente aí que a privacidade assume seu valor, sendo inclusive para alguns o direito inicial, constitutivo dos outros direitos, já que a privacidade garante o direito ao eu (*right to the self*). Nessa perspectiva, sem a privacidade seria impossível o desenvolvimento da própria personalidade.

A privacidade, em outras abordagens, é definida como algo da vida íntima, por vezes até relacionado à solidão, ou ao direito ao isolamento. Entretanto, a privacidade não está relacionada apenas ao que ocorre na esfera privada, e a fotografia de celebridades em espaços públicos é um exemplo que remete ao que Warren e Brandeis (1890) já diziam sobre o uso de "dispositivos

modernos de gravação e reprodução de cenas ou sons". A separação entre as esferas público e privada na modernidade influenciou o que se compreende por privacidade.

Ocorre que esta concepção liberal de privacidade não leva em consideração o caráter relacional e contextual do que é privado, ou seja, o que é íntimo, de um lado, e o que é exógeno, de outro (Cohen, 2012; Nissembaum, 2009). Neste sentido, a privacidade se refere às trocas entre o eu e o outro, das fronteiras dessa relação, e não necessariamente a separação do que é público do que é privado.

Nissembaum (2009) questiona se "a privacidade é uma reivindicação, um direito, um interesse, um valor, uma preferência, ou apenas um estado de existência" (p.2). Para a autora predominam duas abordagens com relação à privacidade, um que enfatiza a "restrição de acesso e outra que se caracteriza como uma forma de controle" (Nissembaum 2009, p.69). Na primeira linha estão autores como Gavison (1980), que define privacidade "enquanto a medida de acesso que outras pessoas têm de você por meio de informação, atenção e proximidade física" (*apud* Nissembaum, 2009, p.68). De forma semelhante está a interpretação de Reiman (1976), que indica que a privacidade "é a condição em que outras pessoas estão privadas de acessar informações ou experiências sobre você" (p.30). Por sua vez, para Westin (1967) a privacidade trata-se "da reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida a informação sobre eles é comunicada a outros" (p.7). Todos estes autores partem da restrição ao acesso físico ou informacional para definir a privacidade.

Em outra linha de abordagem, encontram-se os autores que associam a privacidade ao controle sobre as próprias informações. Para Fried (1968), "a privacidade não é simplesmente a ausência de informações sobre nós na mente dos outros, mas é o controle que temos sobre nossa informação" (p.482). Já Allen (1988), por sua vez, vai um pouco além da relação entre controle sobre as informações e destaca que a privacidade envolve três dimensões; a privacidade física, relacionada ao isolamento e solidão, a privacidade informacional, determinada pelo segredo e confidencialidade sobre as informações pessoais e a privacidade de propriedade. Observa-se que esta última abordagem sobre privacidade não está limitada aos aspectos de controle e acesso, agregando a dimensão física e informacional ao conceito. Sendo assim, a autora enfatiza;

> A privacidade está associada a não uma, mas a três dimensões da distinção público/ privado: (1) a dimensão dos atores, dividida entre atores governamentais e privados; (2) a dimensão das esferas, incluindo o espaço, que pode ser dividido em público e privado; e (3) a dimensão da informação, que pode ser dividida entre pública e pessoal. (Nissembaum, 2009, p.102).

Estas três dimensões – atores, esferas e informação – são a base do modelo conceitual de integridade contextual que a autora propõe para abordar a questão. Para ela, existe uma falha em definir a privacidade enquanto um direito positivo associado a autonomia, liberdade e criatividade.

Seu argumento é que as tecnologias da informação e comunicação aumentaram a capacidade de rastreamento, monitoramento, agregação, análise, disseminação e publicação de informações, comprometendo a privacidade. Ressalta que "impulsionados por um alto poder de processamento, técnicas matemáticas e estatísticas cada vez mais sofisticadas tornaram possível extrair significados descritivos e preditivos de informações" (Nissembaum, 2009, p.42), referindo-se a fenômenos como a big data, o *machine learning* e a inteligência artificial dos algoritmos, fundamentais para a consolidação do capitalismo de vigilância.

Conforme enfatizado na primeira parte deste capítulo, os algoritmos são cada vez mais responsáveis por tomar decisões, como o que é visualizado nas redes sociais, no anúncio do buscador, na ordem de vídeos sugeridos, dentre outras escolhas cotidianas realizadas em dispositivos digitais. Nissembaum (2009) destaca que há uma "mudança na natureza da coleta de dados, realizada de forma automatizada e indiscriminada" (p.21). Não se trata mais de uma exposição aos dispositivos eletrônicos, mas de máquinas "aprendendo o que podem sobre as pessoas, seus atributos e ações passadas, em um esforço para entender suas predisposições e prever ações futuras" (Nissembaum, 2009, p. 42). O que remete àquela expressão "como se os loucos estivessem no comando do manicômio", só que, no caso, é a inteligência artificial cada vez mais controlando os dispositivos digitais (Zuboff, 2019). Como são programados para estimular o consumo e conter a atenção dos internautas, estes códigos estão também transformando as relações sociais, dentro e fora da web.

Justamente devido à transição do modelo analógico ao digital de armazenamento de informações, Nissembaum (2009) propõe que as restrições à privacidade sejam observadas a partir do fluxo de informações, dos contextos sociais e das normas informacionais. Em seu modelo, as normas informacionais "se caracterizam por quatro parâmetros chave; contextos, atores, atributos e princípios de transmissão" (Nissembaum, 2009, p. 141). Em sua visão, este modelo situa as restrições à privacidade em fluxos de informação mais complexos, enfatizando que certas informações podem ser cedidas para determinados atores, em circunstâncias específicas. O exemplo do prontuário médico ilustra bem o modelo contextual de privacidade. Os pacientes proveem informações a seus médicos, que possuem o dever ético de mantê-las sob sigilo. A informação é relevante neste contexto, mas não deve ser utilizada para outras finalidades, como, por exemplo, por planos de saúde.

Outra grande contribuição do modelo de integridade contextual de privacidade de Nissembaum (2009) é o foco no fluxo de informações. De fato, alguns autores definem privacidade com relação isso, como, por exemplo, Parent (1983) para quem a privacidade é "a condição de outros não terem acesso ao conhecimento pessoal sobre alguém. A privacidade de uma pessoa se reduz exatamente na medida em que outros possuem esse tipo de conhecimento sobre elas" (p. 269). De forma semelhante, Cohen (2012) se refere a uma privacidade informacional determinando-a como a capacidade de "manter fora da visão do público certos fatos pessoais, íntimos" (p.178). De forma

ainda mais abrangente Van den Hoven (1999) defende que a privacidade deve ser protegida devido a quatro questões; “(1) danos baseados na informação, (2) desigualdade informacional, (3) injustiça informacional e (4) invasão na autonomia moral” (p.433). Para o autor, danos baseados na informação se referem ao roubo de identidade, mas também a divulgação de informações sem consentimento, como por exemplo, telefones pessoais divulgados em sites da Internet.

Por sua vez, a desigualdade informacional ocorre quando os fluxos de informações pessoais não são sistematicamente limitados, beneficiando de forma desproporcional algumas partes em relação à outras, como se observa no fenômeno de venda de dados pessoais. Já a injustiça informacional está relacionada à quando a informação não fica em sua esfera apropriada, o que pode gerar uma série de danos, que envolvem desde a não concessão de planos de saúde devido ao conhecimento sobre dados de saúde das pessoas, à recusa de crédito devido ao acesso indevido a informações bancárias, dentre outras.

Por fim, com relação à autonomia moral Van den Hoven (1999) destaca que se trata “da capacidade de moldar nossas próprias biografias, refletir sobre nossas carreiras, avaliar e identificar nossas escolhas, sem o olhar crítico e a interferência de outros e a pressão para se adequar às identidades "normais" ou socialmente desejadas” (p. 439), conceito que se aproxima ao de autonomia decisória (Cohen, 2012). Esta autora destaca como a noção de privacidade ampliou-se para além da conexão com a propriedade privada e a família patriarcal, passando a incorporar também “as noções de inviolabilidade da personalidade, de intimidade, e de integridade corporal” (p. 173). Cohen (2012) enfatiza a importância da privacidade na formação da própria identidade e na possibilidade de construção de uma autonomia decisória. Para ela “a privacidade como autonomia decisória libera o indivíduo da pressão para adotar, como suas próprias, as razões que "todo mundo" aceita” (Cohen, 2012 p. 193). Ou seja, a incorporação do pensamento hegemônico como única alternativa. Com a ampliação dos direitos individuais e o reconhecimento da pluralidade das sociedades contemporâneas, o direito à privacidade “tem um papel importante na proteção das capacidades dos indivíduos para formar, manter e apresentar aos outros uma auto concepção coerente, autêntica e distinta” (Cohen, 2012, p. 188). Neste sentido, a privacidade é constitutiva da autonomia nas sociedades liberais e requer espaço íntimo para se desenvolver.

De fato, a noção de intimidade concerne à relação de uns com os outros, ou à natureza das relações entre as pessoas (Nissembaum, 2009). Ela pode ser compreendida como o sentimento ou atmosfera de proximidade com relação aos outros, não necessariamente vinculado à esfera privada. É fundamental não apenas para a construção das identidades, como também é determinante da fronteira do que é privado. Informações como orientação sexual, religião, hábitos de consumo, dentre outras questões pessoais e são consideradas íntimas, ou do âmbito privado. Neste sentido o direito à privacidade é fundamental, pois oferece “precondições constitutivas mínimas para que se tenha uma

identidade própria" (Cohen, 2012, p.188). Portanto, observa-se uma estreita ligação entre a privacidade, a autonomia e o desenvolvimento da própria personalidade. Sendo assim, ainda que existam críticas ao modelo liberal de autonomia, trata-se de um valor que se solidificou nas sociedades ocidentais como constitutivo do próprio ser. É neste contexto que a privacidade se torna necessária para o desenvolvimento da própria autonomia.

Nissembaum propõe ainda uma discussão sobre a questão da privacidade em público. Em trabalhos anteriores (Nissembaum, 1997; Nissembaum, 1998) ela problematizou a instalação de câmeras de segurança em grandes cidades do mundo e o mapeamento realizado pela ferramenta *Google Street View*, que permite a navegação em espaços públicos por meio da Internet.

Este último caso é especialmente emblemático, pois diante das pressões sociais o Google teve que mudar sua política de privacidade. Lançado em 2007, a ferramenta utilizou carros equipados com câmeras de fotografia para registrar imagens das ruas. Entretanto, ao fazê-lo também fotografou pessoas passando, placas de carro, assim como outras informações presentes no espaço público que, podem ser consideradas como privadas. Inicialmente, o Google se negou a retirar da ferramenta imagens identificáveis (especialmente de pessoas), alegando que elas foram capturadas no espaço público (Nissembaum, 2009, p.216). Entretanto, cerca de um ano após seu lançamento, a empresa cedeu[23] às críticas e desenvolveu um algoritmo que transforma rostos e outras informações consideradas como sensíveis em borrões.

Neste contexto, observa-se o fato de que a publicidade – no sentido de transparência - deixa de ser contextual e torna-se ampliada. Existe uma diferença entre falar em público na rua e ter esta fala transmitida ao vivo pela Internet, em tempo real, para uma audiência indeterminada. De forma semelhante, estar na rua e ser gravado pelo *Google Street View,* ou por câmeras de segurança, torna a experiência de estar em público uma exposição constante, onde tudo é gravado e registrado.

O debate sobre sistemas de vigilância e a privacidade em púbico ressalta um aspecto coletivo da privacidade que muitas vezes é negligenciado. Regan (1995) argumenta que a privacidade não deve estar associada a interesses individuais e aponta que se deve reconhecer a importância da privacidade enquanto um valor comum, público e coletivo (p.221). A autora aponta como o direito à privacidade está associado aos valores liberais, tais como a liberdade de expressão e de associação, sendo constituinte também do sistema eleitoral/representativo ao instituir o voto secreto. Além disso, "ao promover a privacidade como um bem coletivo, Regan invoca ainda uma dimensão social, a da privacidade como um bem coletivo indivisível e não exclusivo" (Nissembaum, 2009, p.87). Nesta

[23] Google begins blurring faces in Street View. Disponível em < https://www.cnet.com/news/google-begins-blurring-faces-in-street-view/ >. Acessado em 11/1/18,

perspectiva a privacidade não seria apenas um direito individual, tornando-se alvo de um outro modelo de regulação.

De forma semelhante, Zuboff (2019) enfatiza a dimensão coletiva do tratamento das informações pessoais. Para ela os algoritmos inteligentes evoluíram da compreensão do indivíduo para populações. O exemplo mais contundente disso são as propostas de cidades inteligentes (*smart cities*), que seriam uma evolução do espaço urbano. Os dados coletados pelos mais diversos tipos de sensores gerenciam recursos públicos, a partir de sistemas de vigilância cada vez mais complexos.

Justamente por isso, "devido a mudanças radicais na capacidade de realizar a vigilância, tornou-se necessário proteger a privacidade mesmo em público. Endossando essa conclusão (...) se rompe a relação da privacidade exclusivamente com o privado" (Nissembaum, 2009, p.119). Portanto, cada vez mais é preciso abordar a privacidade de uma perspectiva coletiva, não apenas como um direito individual.

A partir desta contextualização sobre o conceito de privacidade discute-se sua relação com outros valores do pensamento político contemporâneo tais como; autonomia, transparência, segurança e liberdade. Conforme discutido nas últimas páginas a privacidade pode ser definida a partir do acesso ao eu, como também por meio do controle sobre a própria informação. Está relacionada ainda à propriedade privada, ainda que tenha um caráter coletivo. Se refere ainda à intimidade, a autonomia e ao exercício da liberdade. A seguir explora-se algumas das dimensões da privacidade com relação a outros valores, para em seguida, focar em seu aspecto informacional a partir do debate sobre a proteção de dados pessoais.

1.2.1 - Privacidade e autonomia

A etimologia da palavra autonomia tem origem grega, sendo a junção de *auto* – de si mesmo – e *nomos* – lei – ou seja, aquele que determina suas próprias leis. É um conceito central para a ciência política, mas também para a filosofia e outras áreas do conhecimento. Está relacionado ao conceito de liberdade, independência, autossuficiência, autodeterminação e à própria intimidade. Não se pretende aqui esgotar as disputas em torno do conceito de autonomia, mas é importante pontuar diferentes visões expressas acerca deste valor nas abordagens das teorias da democracia.

O valor da autonomia ganhou muito destaque no pensamento liberal clássico dos séculos XVII ao XIX devido à centralidade das escolhas individuais, mas também devido aos debates sobre a autonomia da igreja e do Estado. Neste sentido autonomia está relacionada ao território, ou seja, a independência dos Estados liberais em criarem as próprias leis, soberanos com relação à religião.

Por sua vez, a ideia do sujeito autônomo liberal está associada à questão da propriedade privada masculina, ou seja, "o status de homem privado que combina o papel de dono de mercadorias

com o de pai de família, o de proprietário com o de 'homem' simplesmente" (Habermas, 1984, p. 44). Sujeito soberano também para escolher a própria religião. Neste contexto a autonomia se refere à liberdade negativa da não intervenção do Estado na vida privada dos homens, e consequentemente "está associada a uma entidade, a família, que serve de proteção a suas relações íntimas 'naturais' contra a intervenção e o escrutínio públicos" (Cohen, 2012, p. 174). Sendo assim, autores do pensamento liberal clássico formularam sua compreensão do valor da autonomia enquanto o exercício e a garantia da liberdade dos homens, sem considerar o contexto social e político necessário para que ela seja exercida por todos os cidadãos de um Estado democrático (Berlin, 1959; Mill, 1995). A principal crítica a universalização do conceito de autonomia é que sua abstração não leva em consideração a assimetria de recursos presente na sociedade, ou seja, não considera o contexto em que as escolhas são feitas.

Em contraposição, a teoria feminista aponta que existem condições sociais que influenciam o exercício da autonomia e a própria cidadania, em especial situações de opressão e dominação, consequentes das hierarquias e relações de poder (Young, 1990; Pateman, 1993). O debate nesta corrente se dá a partir da "análise de quais são e como funcionam as barreiras efetivas ao exercício da autonomia e como análise dos incentivos e formas de tolerância social à subordinação" (Biroli, 2013, p. 32). Esta perspectiva agrega à liberdade negativa não apenas os elementos de opressão e dominação, como também as relações de poder, os processos de formação das identidades, das preferências e a questão da autodeterminação. Sendo assim, o exercício da autonomia deve ser visto também a partir da ótica da formação das preferências, influenciadas por relações de poder e hierarquia, mas também do direito à privacidade, enquanto condição para o exercício da autodeterminação.

Antes de prosseguir, é importante pontuar que "as preferências não são fixas e estáveis, mas são, em lugar disso, adaptáveis a uma ampla gama de fatores" (Sunstein, 2009, p. 221). Desta forma, as escolhas se caracterizam por decisões pontuais, enquanto as preferências são processos mais profundos, que envolvem diversas motivações. De fato, estão relacionadas a padrões de socialização e "a recursos materiais e simbólicos e às variantes institucionais" (Biroli, 2013, p. 57). Consequentemente, as decisões estão sujeitas às "relações de dominação, que operam tanto sobre as possibilidades de comportamento efetivo, quanto sobre os processos de formação das preferências" (Miguel, p. 602, 2015). Em suma, o valor da autonomia não pode ser compreendido a partir de uma visão da simples possibilidade de exercício da liberdade negativa, sem que seja levado em conta o contexto, as formas de opressão e dominação e as relações de poder presentes na sociedade.

Neste contexto é preciso fazer uma distinção analítica sobre dominação e opressão. Para Weber (1991) a dominação é "a possibilidade de impor ao comportamento de terceiros a vontade própria" (p.188), ou seja, o impedimento de decisões autônomas. A opressão, por sua vez, em suas

cinco ou mais facetas, seria a imposição de condições instrumentais que limitam a capacidade de um indivíduo de desenvolver-se, tornando-o mais vulnerável em determinadas situações (Young, 1990). Neste sentido, a opressão seria uma forma de coerção, de impedimento do exercício da autonomia, realizada por agentes externos.

Por sua vez, a dominação é uma forma específica de poder, caracterizando-se como um exercício assimétrico de autoridade por parte de um agente que controla os recursos, materiais ou simbólicos (Pettit, 1997). Os dominados estariam submetidos a comportamentos que beneficiam os que detêm o poder (Miguel, 2018). Neste contexto, os detentores de poder controlariam os mecanismos materiais e simbólicos e a assimetria dessa relação refletiria a dominação. Nesta perspectiva os sujeitos teriam sua autonomia constrangida, em especial por valores socialmente construídos, já que toda preferência é socialmente produzida (Miguel, 2018). Estaríamos vivenciando a incorporação do ponto de vista do dominante, legitimando as hierarquias sociais, por meio do campo simbólico (Bourdieu, 2007).

Feitas estas considerações sobre a distinção entre opressão e dominação, retoma-se o que está no centro do debate nesta seção; a relação entre a privacidade a autonomia. Nas sociedades contemporâneas é inquestionável o fato de que "o exercício da autonomia requer um espaço de liberdade pessoal" (Miguel, 2015, p. 604), seja ele compreendido como intimidade, ou como privacidade. Sendo assim, o exercício da autonomia está profundamente associado à liberdade de escolhas, ou seja, no livre arbítrio, conceito este que está relacionado a discussões teológicas, morais e filosóficas. Isto quer dizer que a noção de autonomia é altamente polissêmica e se modifica de acordo com o contexto social, histórico e cultural.

Por conseguinte, a autonomia está relacionada tanto à formação das preferências como a capacidade em exercer escolhas, sem sofrer algum tipo de coerção. Entretanto, não pode ser reduzida à oposição entre escolhas voluntárias e constrangimentos. Pois, para compreender como se constitui um sujeito autônomo, é preciso "saber quais são os recursos, materiais e simbólicos, disponíveis no processo em que os indivíduos se constituem como sujeitos de suas vidas" (Biroli. 2016, p. 44). Deslocar o foco desta oposição significa compreender que as escolhas não são feitas apenas a partir de uma perspectiva em que cada indivíduo toma decisões racionais com base nos recursos disponíveis. Até porque, em determinadas situações, como na infância e em casos de doença mental, existe certa hegemonia no pensamento social contemporâneo de que os sujeitos não estão aptos a tomarem as melhores decisões sobre suas próprias vidas. A mesma linha de raciocínio está presente em discussões sobre o consumo de drogas e a violência doméstica, por exemplo, pois amplia-se o entendimento ao partir da perspectiva de que "não são as escolhas dos indivíduos, mas as condições em que elas se dão que ganham centralidade" (Biroli, 2016, p.44). Sendo assim, existem outros elementos que devem ser considerados sobre a conjuntura em que as decisões são tomadas, já que os

processos decisórios são ainda caracterizados por suas maleabilidades, contradições, circunstâncias sociais, escolhas anteriores e opções disponíveis (Benkler *et all*, 2018).

A privacidade torna-se condição de existência do individualismo ético que está no coração do liberalismo. Como imaginar neste contexto que as pessoas renunciem à privacidade em troca de alguns produtos e serviços gratuitos oferecidos pelas tecnologias da informação e comunicação? Ao longo das próximas páginas, desenvolve-se este debate a partir da problematização de teorias da vigilância, que partem da premissa de que os algoritmos possuem a capacidade de moldar comportamentos. Argumenta-se que a falta de transparência sobre seu funcionamento não permite realizar aferições exatas sobre estas possibilidades e que existem outros elementos que precisam ser levados em conta. Indica-se como solução a necessidade de regular os próprios algoritmos como forma da própria proteção de dados pessoais.

Em primeiro lugar, quando se fala em autonomia no ambiente digital é central compreender que se trata de um espaço regido por códigos binários. Sujeitos autônomos necessitam de informação para acessarem as possibilidades que determinam suas escolhas, sendo assim, na Internet e em outros ambientes digitais é fundamental ao cesso aos códigos e algoritmos que determinam seu funcionamento. Sistemas fechados são como uma caixa preta "em que os participantes da cultura ignoram o interior do que manejam" (Flusser, 2002, p. 113). Em outras palavras, é condição *sine qua non* para o exercício da autonomia em ambientes digitais o acesso às informações, protocolos e os algoritmos que os constituem. O desconhecimento da maneira como operam os códigos que regem a web, colocam sociedade em rede sujeita às mais variadas formas de opressão e dominação, como o controle, a censura e vigilância, seja por parte de corporações, ou por parte de governos. Por isso, são fundamentais iniciativas articuladas de abertura de códigos como o software livre, que possibilitaram o surgimento de práticas de resistência e subversão como *hackers*, *cypherpunks*[24], ciberfeministas, dentre outros, ainda que existam limites à estas iniciativas.

Para finalizar esta seção sobre o valor da autonomia e o direito à privacidade é importante apresentar o debate sobre behaviorismo radical no contexto dos estudos de vigilância. Zuboff (2019), dentre outros autores, parte da premissa de que os algoritmos inteligentes possuem uma capacidade de predição, ou seja, de prever comportamentos para tentar moldá-los. Essa linha teórica defende que a mídia direcionada, todo o sistema de sugestões e indicações da interação da web atuaria diretamente na autonomia dos indivíduos, que poucas saídas teriam diante da capacidade de dominação destas empresas e seus códigos.

Primeiramente é preciso reconhecer que os algoritmos inteligentes se caracterizam pela

[24] Cypherpunks manifesto. Disponível em <http://www.activism.net/cypherpunk/manifesto.html>. Acessado em 12/06/2016.

intenção de se colocarem como intermediários no processo decisivo, ao apontar sugestões, tentar direcionar tendências. Por outro lado, não se pode inferir que os códigos destas plataformas são determinantes nas escolhas individuais por uma série de fatores discutidos a seguir. O que não significa que os efeitos das previsões dos algoritmos não tenham efeitos na sociedade já que eles são instrumentos pelos quais as empresas materializam seus objetivos comerciais.

Para a Zuboff (2019), a mídia direcionada, os assistentes digitais personalizados da Internet das coisas, e todos objetos "inteligentes" influenciam o cotidiano e induzem comportamentos, consumos e preferências das pessoas. Neste contexto é importante ressaltar que a segunda fase do capitalismo de vigilância está marcada pela expansão das tecnologias móveis e de geolocalização que reforçam o importante debate sobre o poder de influência dos algoritmos no comportamento social. É marcada também pela cultura do compartilhamento, ancorada na publicização das experiências privadas, em que ocorre um processo de autoafirmação, em que a exposição da intimidade opera como um reforço da identidade, sendo ao mesmo tempo performática e participativa (Bruno, 2008; Lyon, 2017; Papacharissi, 2015). A extração de dados é facilitada e abre espaço para um segundo momento da mídia direcionada, caracterizada pelo avanço e emprego de algoritmos inteligentes na exploração do estado emocional das pessoas.

O ponto em questão é que não se trata de uma vigilância verticalizada, realizada por parte do Estado, ou por corporações de tecnologia, mas um monitoramento automatizado realizado por algoritmos inteligentes. A vigilância digital é mais próxima do modelo de sociedade de controle de Deleuze (2006), que a enxerga diluída na sociedade. Entretanto, a experiência vivida na sociedade contemporânea não se caracteriza apenas pelo controle, pela divisão entre os vigiados e os que vigiam, ou pela assimetria de conhecimento sobre o que ocorre. A vigilância acaba por ser "útil" para o cotidiano das pessoas e por isso ela não é percebida como intrusiva, controladora ou punitiva.

É neste sentido que Deleuze (2006) empregou a noção de modulação para descrever a mudança das sociedades disciplinares para sociedades de controle. Para o autor o indivíduo tornou-se divisível ao passo que o marketing se tornou um instrumento de controle social (2006). É relevante esta observação sobre a divisibilidade do indivíduo; somos ao mesmo tempo muitas coisas, dentre elas consumidores, trabalhadores, cidadãos, enfim, seres imersos em uma complexa malha de relações sociais caracterizada por preferências adaptativas (Sunstein, 2009). Para Deleuze (2006), a modulação opera como uma forma de controle, em um novo regime de dominação. Ou seja, a cada molde social que o indivíduo tem que se adaptar é uma forma de exercício de controle. Neste sentido, observa-se uma convergência com o pensamento de Foucault (2012) em que a vigilância é mais produtiva no sentido de fabricar comportamentos desejados do que punitiva.

Ancorando-se no conceito de modulação de Deleuze (2006), diferentes autores caracterizam os algoritmos inteligentes como agentes de modulação do comportamento. Para eles (Zuboff, 2019.

Bruno, 2008; Silveira, 2017) estes códigos estão embutidos com uma característica performática, ao modelar dinâmicas, práticas e comportamentos. As mídias sociais, em especial aquelas que ancoram a experiência de uso nas emoções, estariam exercendo o paradoxo da liberdade controlada, ou seja, a capacidade de se expressar de acordo com parâmetros já definidos. A modulação comportamental dos algoritmos inteligentes se daria, portanto, justamente pela sensação de liberdade sob certas restrições, em que se compreende "os algoritmos como atores performativos e o usuário como um agente ativo, não passivo, nessa interação" (Machado, 2018, p. 18). Assim como o Google em seus estágios iniciais, quando seus algoritmos aprendiam a partir do uso que as pessoas faziam de seu buscador, os códigos do Facebook e outras plataformas estariam em constante "diálogo" com as pessoas, empregando determinadas decisões a partir de ações de cada um dos indivíduos. Conforme já mencionado é justamente este o campo de atuação do design de interação, o que não significa atuar para moldar comportamentos.

É neste contexto que se destaca algumas ressalvas a serem consideradas quando se discute a capacidade de dominação das tecnologias da informação e seus algoritmos inteligentes em prever e moldar comportamentos, como defendem os behavioristas radicais. Primeiramente, o fato é que como os algoritmos são patenteados não se pode inferir sobre suas características e potencialidades de predição com exatidão. Entretanto isso não significa que esta tentativa de modulação não tenha efeitos na sociedade. Em segundo lugar, visões determinísticas de que a sociedade está subjugada às novas tecnologias da informação ignoram a capacidade de resistência e de questionamento características dos seres humanos, mesmo que limitadas. Não leva em consideração que as pessoas também podem manipular as máquinas de forma subversiva, ou que podem encontrar formas alternativas de lidar com o capitalismo de vigilância. Somado à capacidade de resistência dos seres humanos há de se considerar também o fato de que as preferências não são fixas e sim maleáveis (Sunstein, 2009). São processos dinâmicos em que as sugestões dos algoritmos podem ora fazer sentido, ou indicar absurdos e contradições.

Em terceiro lugar, é preciso considerar que para que a dominação persista é necessário que haja certa permissividade e conformidade dos dominados (Miguel, 2018). Neste sentido, ainda que a sensação de impotência individual diante dos gigantes de tecnologia esteja presente, há de se lembrar que existem instituições globais que combatem o tratamento indiscriminado de dados pessoais. Por mais que pessoas se acomodem, há um Regulamento Geral sobre a Proteção de Dados vigente. Tribunais, conselhos, autoridades, entre outros, atuam para transformar o modelo de negócios das empresas. Portanto, a dominação não é exercida verticalmente sem que haja certa resistência, inclusive institucional, o que, novamente, não significa que surtam efeitos na sociedade.

A partir da entrada em vigor do Regulamento Geral sobre a Proteção de Dados, as pessoas ganharam uma margem de negociação com estas empresas, em especial a partir da revisão dos termos

de uso destas plataformas. Estes contratos se caracterizam como consentimentos pouco esclarecidos, inclusive realizados em condições que limitam o exercício da liberdade, dos direitos e de relações mais autônomas (Pateman, 1993). As pessoas aceitam os termos de uso sem compreender bem o que será feito com suas informações pessoais, em troca de um serviço gratuito, ou o uso de um aplicativo. O consentimento inicial é seguido de interferências arbitrárias – uma sugestão não solicitada, uma indicação de amizade de alguém que a pessoa odeia. As empresas de tecnologia constrangem as pessoas em aceitarem seus termos de uso. É neste contexto que se questiona a presença do consentimento explicito em acatar estes contratos. O aceite dos termos de uso das plataformas digitais está longe de ser voluntário, esclarecido e autônomo. Justamente por isso, o Regulamento Geral sobre a Proteção de Dados impõe limites e restrições nestes acordos, além de estabelecer o direito da pessoa em suspender o contrato quando quiser, reforçando sua autonomia.

Entretanto, o marco regulatório sobre proteção de dados pessoais, detalhado nos próximos capítulos, não é suficiente para conter o monitoramento automatizado das experiências pessoais. A falta de transparência sobre o funcionamento dos algoritmos não permite que se afirme sobre sua capacidade de influenciar ou não, comportamentos. Por outro lado, é necessário reconhecer que o fato de não ser possível inferir sobre a capacidade de modulação dos algoritmos não significa que sua atuação não tenha efeitos na sociedade. Mas existe uma diferença entre detectar comportamentos e tendências e manipulá-los, já que as pessoas possuem outros estímulos e bagagens.

Neste debate há de se considerar que o exercício do poder é diferente de sua capacidade de influência. A intenção não significa realização. É reconhecível que existe a motivação de influenciar comportamentos, hábitos de consumo, preferências políticas e que isto tem efeitos sociais complexos. Entretanto, como destaca Benkler *et all* (2018), é um erro de diagnóstico apontar as tecnologias como manipuladoras responsáveis por fenômenos como a polarização política. É necessário observar toda a conformação do espectro eletromagnético e a infraestrutura de comunicação, historicamente constituída pelo setor privado e marcadamente pouco plural.

Para se compreender como o fenômeno de monitoramento automatizado das experiências privadas realizado por algoritmos inteligentes, com intenção de induzir ou direcionar a certos comportamentos, de fato afeta as pessoas e a sociedade, seria necessário regular os algoritmos inteligentes. Compreender como funcionam é central para inferir sobre seus impactos nas sociedades, ainda que a simples abertura dos códigos não signifique que seja possível controlar seus efeitos. Mas a transparência sobre como operam os algoritmos é complementar ao debate sobre proteção de dados pessoais e privacidade. Os algoritmos não são neutros, são instrumentos que operam de acordo com finalidades pré determinadas. Justamente por isso suas decisões não são tomadas com base em análises isentas ou critérios de justiça, mas operadas de acordo com interesses, em sua maioria comerciais. Por isso, a urgência de haver transparência sobre a forma que operam, em especial quando

as pessoas estão sujeitas às decisões tomadas por eles. Entretanto o simples acesso aos códigos não é suficiente para controlar seus efeitos na sociedade. A transparência é apenas um passo para compreender a complexidade de suas repercussões.

Tutt (2017), que é advogado do Departamento de Justiça do governo dos Estados Unidos, defende um modelo regulatório para os algoritmos nos moldes da agência nacional do Departamento de Saúde e Serviços Humanos, a *Food and Drug Administration* (FDA). Ele descreve como a autarquia foi criada diante de uma crise sem precedentes de saúde pública, em 1906 (Tutt, 2017, p.120). Para o autor, dentre os modelos regulatórios existentes no país este seria o mais adequado. O fato é que a necessidade de regulação dos algoritmos é cada vez mais urgente. Dado a centralidade que o princípio da transparência possui no debate sobre algoritmos, democracia e privacidade dedica-se a próxima seção do trabalho para caracterizar este conceito, além de problematizá-lo a partir da discussão sobre a conformação do neoliberalismo.

1.2.2 - Privacidade e transparência

Nesta seção trabalha-se com a relação entre privacidade e transparência, compreendidas como opostas na contemporaneidade a partir da máxima *cypherpunk* "privacidade para os fracos e transparência para os fortes" (Assange, 2013), ou seja, proteção aos cidadãos e controle social para governos e empresas. Além de resgatar o histórico do conceito é realizada uma importante contextualização sobre seu emprego em defesa do neoliberalismo. Discute-se a importância dos dados abertos para aumentar o controle social e a transparência dos Estados, responsáveis por garantir a privacidade de seus cidadãos. Finaliza-se enfatizando a importância da aplicação deste princípio na regulação dos algoritmos.

O conceito de transparência é relativamente novo no pensamento social e está historicamente associado à ideia de publicidade, cujos debates têm origem na filosofia política e na própria constituição do Estado moderno. Durante o Iluminismo, pensadores e filósofos da elite europeia enalteciam o conhecimento e a razão como uma forma de libertação, já que a compreensão sobre os fenômenos significava também um domínio maior sobre eles. O movimento marca o fim da idade média e do Estado absolutista, consequentemente influenciando os debates que viriam a conformar as democracias liberais da atualidade.

O filósofo alemão Immanuel Kant foi o primeiro a utilizar o conceito de *Publizität* para designar a qualidade do que é público e relacioná-lo à justiça. Para ele "são injustas todas as ações que se referem ao direito de outros homens cujos princípios não suportam a publicação" (Kant, 2004, p. 165). O que não pode ser submetido ao domínio e conhecimento público tende a ser injusto. Sendo assim, sua concepção de publicidade está diretamente relacionada às condutas idôneas, ao que é de

interesse público, da conformação de uma sociedade em que o saber é importante. Para o pensador, aquilo que permanece oculto, ou em segredo, tem a tendência de ser injusto. Trata-se de uma questão ética; as regras, normas, ou decisões que dependem do segredo, não são moralmente satisfatórias.

Mas é com o jurista inglês Jeremy Bentham, contemporâneo de Kant, que o conceito de publicidade ganha a conotação atual. Para ele a publicidade era uma forma de garantir que o poder do Estado não fosse desviado do interesse geral, prevenindo o abuso de poder por parte dos entes públicos. Para o autor, a publicidade era capaz de estabilizar as relações políticas em um sistema democrático, já que, em sua visão, ela traria como consequência a legitimidade (Silva, 2016, p.30). A publicidade desempenha ainda papel na relação entre representantes e representados, já que, por meio dela, seria possível conhecer as demandas dos eleitores e, ao mesmo tempo, compelir os representantes a exercerem seu poder de encaminhar os pleitos da população. Por isso, Bentham associava a publicidade ao bom funcionamento do próprio Estado. Nesta visão utilitarista a publicidade opera como um constrangimento (Gomes *et al*, 2018).

De forma que se destacam três dimensões da publicidade; responsabilização das autoridades, valorização do interesse geral dos cidadãos, visibilidade dos atos dos agentes públicos (Gomes *et al* 2018). Estas dimensões sustentam as bases do pensamento liberal de que o Estado só é legítimo quando seu domínio é exercido a partir do consentimento dos governados. Apenas pelo acordo expresso dos cidadãos, o Estado pode intervir na esfera privada. Trata-se, portanto, de uma teoria do Estado moderno em que a administração é governada por lei e seus agentes precisam adotar condutas idôneas, pois estão sujeitos ao escrutínio público.

Longe de esgotar o debate sobre a conformação do pensamento liberal clássico, que permeia todo o trabalho, no momento é importante enfatizar que é o liberalismo que se contrapõe aos Estados absolutistas, em que o segredo é uma forma de dominação política e exercício de poder. É a partir do conceito de publicidade que se compreende que assuntos de interesse público não devem ocorrer em sigilo. Sendo assim, a publicidade, assim como a privacidade, é um conceito fundador do próprio pensamento liberal, e a recusa em sua adoção, ou tentativas de impor sigilos ao que é de interesse público, representa uma contradição com relação à esta teoria política.

No âmbito da administração pública a publicidade envolve a divulgação dos atos administrativos praticados. A passagem da publicidade para a transparência ocorre durante a década de 1990, a partir especialmente de dois documentos; primeiramente no *Cadbury Report*, intitulado – Aspectos Financeiros da Governança Corporativa - na Inglaterra, em 1992. Posteriormente, estes aspectos da governança corporativa são expandidos para os governos a partir dos Princípios da Organização para a Cooperação e Desenvolvimento Económico (OCDE), sobre o Governo das Sociedades, publicado em 1999.

Nestas referências iniciais, a transparência ganha conotações mais amplas que a simples

publicidade; englobaria todo o sistema de freios e contrapesos de Montesquieu, a partir das instituições de controle interno e a divisão dos poderes. Além disso, caracterizaria governos "responsáveis" – que não têm nada a esconder – servindo assim como uma forma de combate a corrupção. Ademais incorporariam a participação social a partir da fiscalização realizada pela população na forma como o próprio Estado opera. A transparência surge, portanto, como um verbete neoliberal, que auxiliaria o bom funcionamento das próprias democracias contemporâneas.

Antes de prosseguir debatendo o conceito de transparência é necessário analisar o termo governança, responsável por introduzir e ampliar seu entendimento. Importado da área de administração de empresas – governança corporativa – a expressão descreve uma nova forma de governabilidade imposta pelo neoliberalismo, em que os processos decisórios envolvem cada vez mais o setor privado. A governança pode ser compreendida também como a coprodução público privada das normas internacionais em políticas de integração nacionais, ou regionais ao mercado mundial globalizado, ou uma adaptação do Estado à nova realidade neoliberal (Dardot e Laval, 2016, p. 277). O termo expõe a dependência dos Estados do poder corporativo privado, em especial do mercado financeiro, na expansão do neoliberalismo pelo mundo.

Para Dardot e Laval (2016) o neoliberalismo não é uma ideologia, mas sim uma "ordem prática", ou uma nova racionalidade, que representa o esgotamento da democracia liberal – ainda que o conceito esteja em constante disputa - já que a economia é que orienta a política e não o contrário. Para os autores, as características desta nova fase neoliberal podem ser resumidas em quatro aspectos: O mercado como realidade construída; a concorrência como norma; a transformação do Estado em "empresa" e a conformação de "neosujeitos" empreendedores.

Trata-se do fim do pacto de bem-estar social keynesiano entre o capitalismo de mercado e as democracias liberais (Dardot e Laval, 2016). De um lado, os Estados se omitem a regular setores como o tecnológico e o financeiro. De outro, os investimentos sociais passam a ser disciplinados por leis como a brasileira de responsabilidade fiscal, de 2001. A disciplina do orçamento do Estado torna-se uma questão de transparência, de prestação de contas e responsabilização (*accountability*).

Feitas estas importantes ponderações e contextualizações sobre o estabelecimento do conceito de transparência na contemporaneidade é preciso complementar que existem outras concepções de fundo. A primeira delas é a previsibilidade, ou seja, o estabelecimento de regras prévias que possibilitem o controle das condutas. A exigibilidade, por sua vez, se refere ao direito de conhecimento sobre o que afeta a todos. A inteligibilidade das informações, ou seja, a garantia de que serão compreensíveis e, portanto, controláveis e a já discutida publicidade. (Silva, 2016, p. 31).

Dentre os aspectos positivos de iniciativas de transparência destaca-se; o aumento de eficiência das instituições, a diminuição dos custos de *accountability*, o incentivo à participação, o aumento de confiança no sistema político e a redução da corrupção. Por outro lado, a transparência

pode refletir em um aumento da desconfiança do público, subestimar o fenômeno da corrupção e gerar um volume de informações que o público não consegue acompanhar (Silva, 2016).

Os mecanismos de transparência, como outros aspectos da vida social, sofreram influência das tecnologias da informação e comunicação. A divulgação dos atos administrativos no modelo analógico tinha suas restrições, barreiras que no universo digital se transformam. O aumento da capacidade de armazenamento e processamento de dados – a *big data* – ampliaria as informações governamentais em iniciativas de transparência digital.

Antes de prosseguir, é importante mencionar que modelos de código aberto são condição *sine qua non* para a transparência digital. Apenas sistemas abertos são transparentes, ao contrário de sistemas proprietários em que a iniciativa privada monopoliza o conhecimento. Iniciativas de governo eletrônico que almejam dar publicidade, inteligibilidade, previsibilidade e exigibilidade a seus sistemas precisam ter seus códigos abertos. Portanto, a transparência digital está intimamente relacionada ao modelo aberto de desenvolvimento do software livre e à própria segurança destes sistemas.

O conceito de dados abertos foi cunhado a partir da expansão da web e da filosofia do software livre, em meados década de 1990. Entretanto, possui tem inspirações anteriores como, por exemplo, a tese do sociólogo estadunidense Robert Merton de que toda pesquisa cientifica que produza dados deve ser compartilhada livremente visando o bem comum. Os dados abertos se caracterizam por licenças livres, que garantem a participação universal, padrões técnicos de interoperabilidade que asseguram a possibilidade reutilização e redistribuição e por sua disponibilidade e acesso. Portanto, os dados abertos se tornam a materialização da transparência pública.

É neste contexto que surge o termo governo aberto, que se caracteriza pela adoção de quatro princípios; a transparência, a prestação de contas e a responsabilização (*accountability*), a participação cidadã e a tecnologia e inovação. É a promessa de uma nova forma de governar, ancorada nas potencialidades da tecnologia e na visão do Estado enquanto empresa, incorporando a eficiência da governança corporativa e a lógica neoliberal. Em 2011, durante a assembleia anual da ONU, é lançada a Parceria pelo Governo Aberto, ou *Open Government Partnership*, iniciativa endossada por 65 países, dentre eles o Brasil, que adotam os princípios do governo aberto.

É neste mesmo período que se consolida a transição do modelo de capitalismo de corporações ao neoliberalismo, marcado pela ausência de regulamentação do setor tecnológico e do mercado financeiro. Além disso, essa mudança tem como característica fundamental a transformação do papel do Estado, que passa a atuar mais em defesa de interesses privados do que na proteção de direitos sociais. Estas novas formas de governo transformam a visão do que é público e privado, do que é político e do que é económico (Harvey, 2008; Brown, 2015; Fraser, 2012; Dardot e Laval, 2016).

Conforme discutido, as iniciativas por mais transparência governamental têm origem no

modelo de governança corporativa, oriundo da administração. Ainda assim, o modelo não é adotado nos códigos dos algoritmos que influenciam o cotidiano das pessoas. Eles funcionam de forma opaca e suas transformações e adaptações são ainda mais obscuras. Ocorre uma transparência da vida cotidiana, a partir da exposição pessoal e a coleta de dados, que não é acompanhada pela divulgação dos códigos, que neste contexto passam a ser de interesse público.

Portanto, a regulação dos algoritmos se torna uma questão de transparência das companhias que detém esses códigos proprietários. É necessário conhecer a forma com que operam para garantir a privacidade, a segurança e a liberdade das pessoas. Utilizando o jargão neoliberal que rege o setor de tecnologia, é preciso implementar uma governança algorítmica. A seguir debate-se a associação entre a privacidade e a segurança, uma falsa dicotomia utilizada para defender políticas de intrusão.

1.2.3 - Privacidade e segurança

Nesta seção discute-se a dualidade entre segurança e privacidade, principal argumento mobilizado para justificar a vigilância. A partir da conceitualização dos parâmetros de segurança, busca-se expor seus diversos aspectos e contrapontos. Em seguida, aprofunda-se o debate sobre o contratualismo, teoria em que a segurança é oferecida em troca da limitação de determinadas liberdades. Aborda-se também os limites do consentimento e a importância e de que ele seja consciente e informado. A partir desse debate teórico, relaciona-se a discussão empiricamente informada com os termos de uso das plataformas de serviços e aplicativos na Internet que correspondem aos contratos realizados entre as grandes empresas de tecnologia e as pessoas. Outro caso empírico tratado nesta seção é o da criptografia. Por fim, enfatiza-se a distinção entre a vigilância de comunicação eletrônica e coleta de informações de inteligência, ambas relacionadas com a questão da privacidade e da segurança.

Em primeiro lugar, o conceito de segurança remete à percepção de estar protegido. Trata-se de uma sensação já que é impossível estar totalmente seguro da principal ameaça; a morte. As pessoas buscam se proteger de riscos, danos, perdas. Existem diversos tipos de segurança; a nacional, do trabalho, da saúde, da informação, a pública e a privada, dentre outras. A seguir aborda-se as mais relevantes para o debate sobre privacidade.

A segurança nacional está diretamente relacionada à ideia de soberania. O Tratado de Vestfália, assinado em 1648, é fundador da noção de que cabe ao Estado proteger a ordem social, dando a ele o monopólio do uso da força dentro de seu território. Também conhecido como a Paz de Vestfália, o tratado determinou ainda o princípio de não intervenção em outros Estados nação, ao estabelecer a igualdade jurídica entre eles e, sobretudo, constituir as fronteiras. Portanto, o Estado é soberano em seu território e não tem o direito de intervir em outros, o que constitui um dos princípios

da diplomacia e das relações internacionais modernas. Algumas limitações do tratado se tornam mais evidentes a partir da a globalização e a expansão das tecnologias da informação e comunicação, já que os limites territoriais não são mais suficientes para que ações perpetradas dentro de um Estado não influenciem diretamente a soberania de outros.

Além disso, a segurança nacional é responsável pela proteção do território de ameaças externas e internas, o que leva à constituição tanto da defesa civil, como aos serviços de inteligência e espionagem, ambos com o objetivo de prevenção. O tema tornou-se central nas últimas décadas em decorrência de ataques como o 11 de setembro nos Estados Unidos, os de 11 de março de 2004, em Madrid e, mais recentemente, os de 13 de novembro de 2015, em Paris. O terrorismo tornou-se assim a principal ameaça à segurança nacional dos Estados nação do norte global. Foi responsável também pela expansão do sistema de inteligência e espionagem, que sempre foi perpetrado pelos Estados, mas que aumenta em termos de escala, ao ponto de investigar presidentes de países considerados "amigos".

Outro tipo de segurança relevante ao debate sobre privacidade é a segurança da informação (Stallings, 2008). Padronizado internacionalmente pela ISO/IEC 17799:2005, a segurança da informação tem como base os princípios de confidencialidade, integridade, disponibilidade e legalidade. A confidencialidade refere-se à limitação do acesso à informação as entidades legítimas, ou autorizadas pelo proprietário da informação. Ou seja, garante que apenas as pessoas autorizadas tenham acesso à informação. Portanto, está diretamente associado ao sigilo ou segredo, sejam eles de estado, de concorrência, ou pessoais.

Por sua vez, a integridade garante que a informação armazenada seja preservada, mantendo suas características originais, sem ser alvo de manipulações. Este princípio está diretamente associado à noção de autenticidade, ou seja, de veracidade. Já a disponibilidade, se refere à característica de ser acessada sempre que necessário pelos agentes autorizados. Tanto a disponibilidade como a confidencialidade se relacionam à legitimidade, já que estabelecem que as informações só podem ser acessadas por pessoas autorizadas, dentro dos limites legais.

Uma importante ferramenta para garantir a segurança da informação é a criptografia. O processo de encriptação é aquele que converte um texto puro em um código cifrado, que só poderá ser desconvertido por agentes autorizados. Na criptografia moderna este processo é mediado por chaves, ou seja, um "segredo" compartilhado apenas entre as pontas do processo comunicativo. É importante destacar que as técnicas de criptografia potencializam a segurança da informação, entretanto não são infalíveis. O acesso às chaves de conversão pode ser obtido por meio de técnicas como cripto análise, ou ataque por força bruta (Stallings, 2008). De forma semelhante à segurança da informação, a criptografia tem como objetivo a confidencialidade e a integridade. A estes princípios adiciona-se a autenticação do remetente e sua irretratabilidade, que se refere a impossibilidade de o

remetente negar a autoria da mensagem.

Realizadas estas conceitualizações principais, no contexto da segurança nacional e a segurança da informação, é preciso destacar a Convenção de Budapeste sobre cibercrimes, assinada em 2001. É o primeiro tratado internacional que se refere a contravenções penais realizadas por meio das tecnologias da informação e comunicação assinado no âmbito do Conselho da Europa. A convenção estabelece formas de cooperação entre as autoridades, harmoniza as legislações nacionais e determina procedimentos investigativos para crimes como spam e malwares, ataques de negação de serviço (DDoS), propagação e discurso de ódio relativo à xenofobia e racismo, violações de direitos autorais e de segurança de redes, dentre outros. Ratificada pelos Estados Unidos em 2006, a convenção opera preservando as obrigações de direitos humanos da União Europeia e estabelece procedimentos para acesso a dados transfronteiriços. Trata-se, portanto, da principal referência internacional sobre cibercrimes e segurança da informação.

Feitas estas considerações sobre o conceito de segurança e os tipos mais relevantes para a questão da privacidade é importante realizar o debate sobre o contratualismo, pois além de sua importância para as teorias da democracia, ele está centrado na ideia de que os sujeitos renunciam a determinadas liberdades justamente para garantir a sensação de proteção e segurança.

Hobbes (1987) é o primeiro grande autor contratualista, sendo referência para diversas correntes das ciências sociais. Para o autor, a sociedade se forma a partir do contrato, já que no estado de natureza impera o conflito e a violência entre indivíduos. Seu argumento é que a ausência de hierarquia é um problema social resolvido a partir do contrato, em que as pessoas renunciam a sua soberania e liberdade em troca da segurança de não sofrerem as brutalidades presentes no estado de natureza. Sendo assim, este contrato de submissão é motivado pelo temor, e tem como objetivo a normalização da violência, levando as pessoas a aceitarem a dominação. É importante destacar que Hobbes (1987) reconhece o papel central do conflito em sua teoria, ainda que sua formulação inicial do contratualismo apresente algumas controvérsias.

Dentre elas, destaca-se que este pacto social, em que as pessoas entregam sua liberdade ao Estado em troca de segurança, parte do princípio de que os direitos individuais são bens alienáveis. Trata-se de uma visão do indivíduo enquanto posse, em uma relação similar com que se tem com bens externos, como a propriedade, por exemplo. Entretanto, a alienação de direitos por meio contratual, que permite a legitimação de relações interpessoais de subordinação, como no trabalho ou no casamento, se dá em uma ordem jurídica em que os direitos são inalienáveis, o que em si já é uma contradição.

Esta questão é colocada por Rousseau (2016), para quem a soberania é inalienável e a instituição do governo não pode ser entendida como um contrato. Ou seja, para o autor não é aceitável um contrato que prive uma das partes da liberdade que ela precisaria ter para entrar nele. Para superar

esta contradição é necessário romper com o individualismo possessivo, noção carregada de dubiedade já que parte da ideia de que há propriedade na pessoa em si, e pensar o direito como usufruto e não como posse. Neste contexto, os termos de uso das plataformas digitais exploram justamente esta fragilidade ao estabelecer a cessão de alguns direitos, ou até mesmo dos próprios dados pessoais.

Outro ponto de fragilidade do contratualismo se refere à entrada e saída deste pacto social. Primeiramente, deve-se levar em consideração que nem todas as pessoas participam desse acordo originário. De fato trata-se de um processo social complexo em que não há um início fixo, ou predeterminado. Em sua formulação inicial, o contrato social se referia a homens com propriedade, excluindo mulheres, crianças e trabalhadores. Somado a isso, é preciso considerar a questão geracional e a inversão na arquitetura da escolha. O indivíduo já nasce no contrato aceitando os benefícios da vida social, portanto a adesão deixa de ser voluntária.

Há de se considerar ainda os altos custos de saída do contrato social e da vida em sociedade. Na Internet o cancelamento da adesão aos termos de uso é conhecido pelo termo *opt out*. Trata-se do direito a romper o contrato quando desejar. Ocorre que os custos da ruptura com serviços hegemônicos de e-mail, mídias sociais, sistema operacional, dentre outras ferramentas digitais é muito alto, pois as opções alternativas são limitadas. O paralelo entre o contratualismo e os termos de uso ilustra como determinados acordos são feitos em condições assimétricas em que as possibilidades de rejeição são muito limitadas.

Feitas estas ponderações, é importante destacar que uma das principais críticas articuladas ao contratualismo é de Patemam (1988). A autora busca investigar formas de submissão naturalizadas na sociedade, entender como são produzidas e questionar seu caráter voluntário. Para ela, a simples anuência não é suficiente para legitimar a dominação que se dá por meio contratual. Portanto, faz-se necessário criar mais exigências para aumentar os critérios de autenticidade das relações de exploração, opressão e violência presentes na sociedade.

Se por um lado, o consentimento na visão liberal é voluntário, esclarecido e autônomo, Pateman (1993) destaca que muitas vezes ele é produzido por condições sociais que impedem relações mais autônomas. Para a autora, o caráter comercial do contrato, cujo modelo é de troca e venda, precisa ser superado, já que sua predominância nas sociedades contemporâneas leva à mercantilização das relações sociais. Esta contribuição é central para o entendimento do contexto atual das democracias concorrenciais, ou seja, o contratualismo está fundado em uma visão econômica e não em princípios éticos de igualdade e justiça.

Por sua vez, Fraser (1992) pondera que, por vezes, os contratos são importantes ferramentas delimitação da subordinação, como, por exemplo, a limitação de horas de trabalho. No caso dos ambientes digitais, os termos de uso poderiam limitar o tratamento de dados. Ocorre que o poder de negociação é muito restrito. Em situações em que a opressão está legitimada a partir da não

interferência do Estado, os sujeitos se veem obrigados a aceitar as condições estabelecidas. Esta ponderação é válida para ambos exemplos citados; o trabalhador desempregado acata condições de trabalho insalubres para não perder a vaga para outra pessoa em condições iguais, ou até piores. Os termos de uso das plataformas já estão redigidos e não apresentam opções para além do "eu concordo". O contrato social em forma de termos de uso apresenta, portanto, os mesmos problemas e limites do contratualismo.

Essa mesma crítica se aplica à dicotomia entre segurança e privacidade. Governos ampliam seus sistemas de vigilância para cidadãos comuns em nome da segurança nacional. Os cidadãos não podem negociar se querem aderir a um Estado de vigilância, renunciando a sua privacidade e liberdade para estarem mais seguros. Entretanto, trata-se de uma abstração da segurança. Para quem ela é garantida? A segurança é igual para todos cidadãos independentemente de sua raça, classe social, e gênero? Portanto, a defesa da vigilância para garantir a segurança reproduz as próprias hierarquias sociais, ao mesmo tempo que suspende a liberdade de indivíduos específicos.

A partir da aparente dualidade entre privacidade e segurança discutiu-se o importante debate das teorias da democracia sobre o contrato social e um paralelo atual, os termos de uso de plataformas e aplicativos digitais. Com isto retomou-se algumas controvérsias associadas a privacidade, proteção de dados, autonomia e segurança. A seguir aprofunda-se algumas questões relacionadas ao exercício de liberdades individuais e da liberdade de expressão.

1.2.4 - Privacidade e liberdade

O conceito de liberdade é debatido desde a antiga Roma por pensadores da filosofia, da ética, das ciências sociais e política. Portanto, poderia ser assunto de uma tese inteira. Reconhecendo desde já que não é o objetivo aqui esgotar o debate sobre liberdade, apresenta-se algumas correntes da teoria política contemporânea importantes para relacionar a liberdade com o conceito de privacidade. A primeira delas é o liberalismo clássico, relevante por sua hegemonia na ciência política contemporânea. A segunda delas, já um contraponto ao pensamento liberal, é o "neo-republicanismo", que relaciona este conceito com implicações práticas da participação política e a própria democracia, englobando assim o debate sobre cidadania. Por fim, é importante abordar também o pensamento marxista, que relaciona a liberdade às condições materiais de existência.

Sendo assim, diante do recorte proposto para o debate não se discutirá a liberdade a partir da perspectiva filosófica, ainda que se reconheça a importância e relevância de autores dessa área, como Jean Paul Sartre e Hannan Arendt, dentre outros. Por outro lado, ao final da sessão, um tipo específico de liberdade será debatido; a liberdade de expressão, já que na atualidade, sem o exercício da privacidade a própria liberdade de expressão é comprometida. Neste contexto o tema do anonimato

também será explorado diante de sua relevância no contexto da Internet.

Antes de prosseguir é importante fazer uma distinção. A palavra liberdade tem origem no latim, entretanto na língua inglesa ela é expressa por dois substantivos; *freedom* e *liberty*. Pitkin (1988) faz justamente esta crítica aos teóricos que compreendem as palavras como sinônimos, reconhecendo Hannan Arendt como uma exceção. Para ela, o substantivo *liberty* refere-se à liberdade de opressão, ou seja, não estar sujeito a um controle externo. Por sua vez, *freedom* estaria relacionado com a possibilidade de participar de assuntos públicos, ou seja, a liberdade política. Esta diferenciação já expõe alguns dos aspectos relacionados ao conceito de liberdade, dentre os quais pode-se incluir outras definições como; a condição de ser livre, a autodeterminação, ou seja, a capacidade de agir por si mesmo, o livre arbítrio, ou até mesmo a ausência de submissão, todas elas associadas ao conceito de autonomia.

A concepção clássica de liberdade engloba estes aspectos, determinando a liberdade negativa como a ausência de coerção e a liberdade positiva enquanto a possibilidade de fazer algo. Trata-se uma perspectiva contratualista, em que existe a premissa de que todas as pessoas nascem livres. Constant (1985) diferencia a liberdade dos antigos e dos modernos. Para ele a liberdade dos gregos era justamente a participação em assuntos públicos. Para os contemporâneos é a possibilidade de obter e desfrutar a riqueza privada, sem sofrer interferências.

Sendo assim, na visão liberal o grande empecilho para o exercício da liberdade é o próprio Estado. Além disso, nesta linha de pensamento as condições materiais e sociais não impactam no exercício da liberdade. Consequentemente, as políticas redistributivas são fazem sentido, pois trata-se de uma questão de mérito individual. É neste sentido que Stuart Mill (1995) defende que o indivíduo é soberano sobre seu corpo, sua mente e si mesmo. É a expressão do utilitarismo, tema ao qual Mill ressalta em outras obras para enfatizar que cada um é o melhor juiz para opinar sobre sua própria vida. O ideal de progresso leva o autor a defender o governo representativo como melhor forma de Estado para sociedades civilizadas, ou seja, aquelas capazes de obedecer às regras. Apenas nestas situações o Estado teria legitimidade para o exercício da autoridade e o constrangimento de liberdades individuais.

Por sua vez, o "neo-republicanismo", em crítica ao pensamento liberal, compreende a liberdade enquanto não dominação. Pettit (1997) resgata uma visão republicana da teoria política, em que a participação cívica nas decisões políticas é a realização da liberdade. Sua teoria remente à visão presente na Grécia antiga sobre cidadania, em que a liberdade é exercida no espaço público, em contraposição ao pensamento liberal, em que a liberdade se realiza no espaço privado. Na perspectiva republicana, a liberdade é a não dominação e não a ausência de interferência, como na visão liberal.

Pettit (1997) destaca alguns aspectos presentes em quaisquer tipos de relação de dominação. Primeiramente “a capacidade de interferência, de forma arbitrária, em certas escolhas que o outro está

em posição de fazer" (p. 52). Sendo assim o exercício da cidadania significa não sofrer arbitrariedades por parte de outros, logo a liberdade política. Ser livre portanto é não estar sob o domínio de outros, não estar na condição de servidão. Sendo assim, o autor desloca o foco da não interferência para a arbitrariedade, ou seja, a ausência de regras. Mas a arbitrariedade não se resume à ausência de regras e a dominação pode ser exercida de forma normativa, no pleno funcionamento das instituições democráticas. Um exemplo disso são os burocratas, que exercem a dominação a partir das regras de forma não arbitrária.

Por sua vez, a teoria marxista possui uma visão distinta das restantes aqui apresentadas, não apenas com relação ao entendimento de liberdade, como sobre a economia política, dentre outras áreas do pensamento social contemporâneo. Longe de esgotar as mais variadas dimensões desta corrente política, no escopo proposto para o debate é preciso destacar que para Marx a liberdade (assim como outras questões) não deveria ser vista como uma questão abstrata. Pelo contrário, só poderia ser compreendida a partir das limitações materiais. Para obter a liberdade seria preciso primeiramente superar as necessidades materiais.

Além disso, a liberdade plena só poderia ser alcançada quando a vida em sociedade não fosse constrangida pelos requerimentos de produção. As limitações não são apenas estas, pois para o autor "é somente na comunidade que o indivíduo tem os meios de desenvolver suas faculdades em todos os sentidos; somente na comunidade, portanto, a liberdade pessoal torna-se possível" (Marx e Engels, 2007, p. 64). Trata-se de uma ruptura com o individualismo liberal, pois para Marx é preciso conviver de forma igualitária em sociedade para desenvolver-se pessoalmente. A teoria marxista expõe a incompatibilidade das democracias representativas – em que a igualdade é uma premissa – com o próprio capitalismo, cuja lógica parte da reprodução das desigualdades.

Outra questão importante que Marx enfatiza é como determinados direitos, dentre eles a liberdade, só são realizados por aqueles que possuem condições materiais para usufruí-los. Ressalta que "nos sucedâneos da comunidade existentes até aqui, no Estado etc., a liberdade pessoal existia apenas para os indivíduos desenvolvidos nas condições da classe dominante e somente na medida em que eram indivíduos dessa classe" (Marx e Engels, 2007, p.64). Com isso o autor expõe o fato de que alguns direitos são privilégios de classe. É conhecida a ausência sobre o debate de gênero no pensamento marxista, mas como apontado pela teoria feminista, estes privilégios são também de gênero, e sua intersecção muitas vezes aprofunda ainda mais as condições de opressão e dominação.

Por sua vez, a liberdade de expressão também é um conceito que data da polis grega, em que os homens livres exerciam sua cidadania ao debater na Ágora. Abrange o entendimento de que as pessoas são livres para se expressar sem sofrer retaliações, censura ou sanção legal. A liberdade de expressão (e de religião) também eram valores da sociedade romana. Foi reconhecida ainda na Declaração dos Direitos do Homem e do Cidadão, da revolução francesa, em 1789, e na Declaração

de Direitos inglesa de 1689. É um direito fundamental reconhecido no artigo 19 da Declaração Universal de direitos humanos, cujo texto ainda garante o acesso à informação.

Está diretamente associada ao próprio conceito de democracia, em que cidadãos são livres para opinar acerca de assuntos de interesse público. De fato, é central para a teoria da democracia deliberativa, em que o debate racional leva à solução de problemas em comum. Entretanto, conforme destacam os elitistas, as opiniões dos cidadãos comuns são pobremente formadas e passíveis de vários tipos de manipulações. Por isso, o sistema representativo seria a melhor forma de conceber uma elite política bem informada capaz de decidir (Mill, 1995). Ao cidadão comum resta a liberdade de expressão e a autorização por meio do voto.

A liberdade de expressão se relaciona ainda à liberdade de imprensa e o próprio conceito de opinião pública (Lippman, 2008). De acordo com esta teoria os meios de comunicação de massa atuam para "traduzir" o mundo para a população em geral. Neste processo decidem quais assuntos devem ter mais destaque no que é conhecido como teoria do agendamento. Parte deste processo editorial consiste ainda no *gatekeeping*, que é a seleção de quais fatos serão ou não noticiados. Há ainda o enquadramento que determina a forma como determinado assunto é informado.

Ocorre que os meios de comunicação de massa, em que a Internet está inserida, consistem em um ecossistema de mídia marcado pela assimetria de recursos e discursos (Benkler *et all*, 2018). Os principais veículos de imprensa estão concentrados em poucos conglomerados, o que afeta a liberdade de expressão a partir do momento em que se reduz a pluralidade dos discursos. A cobertura da mídia muitas vezes acaba por legitimar discursos hegemônicos. Por sua vez, a mídia alternativa atua de forma discreta devido à ausência de recursos. Portanto, a propaganda desempenha papel central neste ecossistema; os anunciantes ainda são o principal público alvo destas empresas, não o cidadão comum. Novamente observa-se a predominância da esfera econômica sobre a política.

Existem limitações ao direito de liberdade de expressão que envolvem crimes, como o racismo, xenofobia, dentre outros, tanto em veículos tradicionais como na web. Ocorre que na Internet, por uma séria de fatores, que vão desde a velocidade com que a informação se propaga, passando pela dificuldade em se identificar o autor original, as limitações clássicas da liberdade de expressão são pouco controláveis. O discurso de ódio, as notícias falsas e a desinformação em geral não são fenômenos que surgiram com a web, mas encontraram nesta ferramenta um meio para se disseminar com mais eficiência.

Neste contexto é importante destacar legislações que buscam garantir a liberdade de expressão online e ao mesmo tempo conter discursos criminosos, como racismo, misoginia, xenofobia, dentre outros. Debate-se muito sobre a responsabilidade das plataformas na disseminação deste tipo de conteúdo. De um lado as empresas se defendem atestando que não podem controlar ou identificar as origens do conteúdo e que as pessoas ao assinarem os termos de uso de seus serviços se

responsabilizam pela autoria daquilo que publicam. Se colocam como meros intermediários do processo comunicativo. Ocorre que como já diria McLuhan (1974) "o meio é a mensagem", ou seja, os intermediários desempenham sim um papel na troca comunicativa.

Justamente por isso, e com o objetivo de conter o discurso de ódio e a desinformação o parlamento alemão aprovou o *Network Enforcement Act* (conhecido como NetzDG), ainda em 2017. A lei estabelece multas para mídias sociais que tenham mais de dois milhões de membros da Alemanha, que sejam ineficientes em remover conteúdos criminosos, em menos de 24 horas. A regulação alemã introduz mecanismos de transparência ao obrigar que as plataformas de conteúdo que recebem mais de cem reclamações publiquem relatórios anuais que detalhem os critérios de moderação de conteúdo. Inclusive, em 2019, o governo alemão multou o Facebook justamente por não cumprir os requerimentos de transparência estabelecidos pela legislação[25].

Este debate permeará boa parte da discussão empírica sobre privacidade e proteção de dados pessoais, no âmbito do Fórum de Governança da Internet. Ainda que a regulação de conteúdo online não signifique o controle do que é publicado, a principal crítica a este tipo de legislação é que as plataformas se tornariam os *gatekeepers* do conteúdo publicado online. Por meio de mecanismos automatizados, estas empresas aplicariam censura prévia a determinados conteúdos, dentre os quais a nudez é o exemplo mais recorrente. Ocorre que, no âmbito da União Europeia, existe o Regulamento Geral sobre a Proteção de Dados, tema aprofundado no próximo capítulo, que permite a revisão não automatizada de decisões tomadas por algoritmos. Isto quer dizer que se uma pessoa tiver um conteúdo retirado do ar que considera legítimo de publicação – como uma mulher amamentando um recém-nascido – ela pode solicitar a revisão da decisão. Com isso, as grandes plataformas precisam contratar milhares de pessoas para rever as decisões automatizadas de seus algoritmos[26].

Longe de esgotar o debate sobre liberdade de expressão, discurso de ódio e disseminação de notícias falsas, uma das principais controvérsias da atualidade, no momento o importante é destacar que existem limitações ao direito de liberdade de expressão. Sobretudo, que este direito não deve ser confundido com a possibilidade de caluniar, difamar, constranger, ou até mesmo tentar licenciar determinados grupos. Justamente por isso, a privacidade é essencial para o exercício da liberdade de expressão, dado que sua ausência pode se tornar um elemento de intimidação e opressão.

Por fim, é importante debater a questão do anonimato, uma forma de liberdade de expressão que busca proteger a fonte das informações, ou seja, mantê-las privadas. A palavra tem origem grega e sua etimologia remonta a noção de "sem nome", não identificável. O anonimato, portanto, dissolve

---

[25] Germany fines Facebook for under-reporting complaints. Disponível em < https://www.reuters.com/article/us-facebook-germany-fine/germany-fines-facebook-for-under-reporting-complaints-idUSKCN1TX1IC >. Acesso em 2/1/20.

[26] Um exército para rastrear o ódio nas redes. Disponível em < https://brasil.elpais.com/brasil/2019/03/22/tecnologia/1553279547_294211.html >. Acesso em 23/9/19.

a personalidade, sendo utilizado em críticas em ambientes hierárquicos com um recurso para manifestar-se sem sofrer retaliações. Justamente por isso, também é um artifício utilizado no exercício de atividades ilegais. Inclusive a Constituição brasileira de 1988 determina que "é livre a manifestação do pensamento, sendo vedado o anonimato". Por outro lado, a primeira emenda da Constituição estadunidense engloba a ideia de anonimato ao proibir o Estado de limitar a liberdade de expressão e de imprensa. Trata-se de uma controvérsia que se encontra inclusive no cerne da estrutura das democracias representativas, em que o voto é anônimo. Por fim, ainda com relação ao anonimato deve-se considerar a assimetria de poder que a identificação possa produzir efeitos negativos para quem se expressa, o que leva à autocensura.

Muitas das discussões apresentadas ao longo deste primeiro capítulo serão retomadas nas próximas páginas a partir da análise empírica em torno do conceito de privacidade e proteção de dados pessoais. Nesta primeira parte do trabalho, desenvolveu-se a argumentação associada aos temas centrais da tese; os algoritmos, a privacidade e teorias da democracia, já que o conceito é polissêmico e possui diversas abordagens. A partir da contextualização e consolidação do fenômeno de monitoramento automatizado realizados por algoritmos inteligentes, conceituado na literatura como capitalismo de vigilância, apresentou-se o problema central da tese sobre o papel dos Estados em regular a proteção de dados pessoais.

No próximo capítulo aprofunda-se na análise dos marcos regulatórios sobre privacidade e proteção de dados pessoais e como eles refletem distintas visões sobre a própria democracia. Em um primeiro momento, analisa-se a legislação do norte global da União Europeia e dos Estados Unidos. Em seguida, avalia-se o caso brasileiro, com a lei geral de proteção de dados.

2 - Proteção de dados pessoais e as democracias do século XXI

No primeiro capítulo do trabalho, discutiu-se a conformação do fenômeno do capitalismo de vigilância e como a privacidade é um conceito do século dezenove, que parece impossível de se realizar no século XXI, em face a expansão das tecnologias da informação e comunicação. Avaliou-se ainda que a privacidade não está associada apenas a metáfora espacial da esfera privada, tratando-se de um conceito subjetivo e relacional (Cohen, 2012; Nissembaum, 2009). Refere-se ao tanto de informação que uma pessoa deseja compartilhar, ou não, com outras. Estas informações pessoais abrangem uma série de dados, por vezes objetivos, como nomes e números, mas também informações comportamentais, conhecimentos culturais, preferências políticas, hábitos de consumo, dentre outros.

Neste capítulo será abordada um aspecto específico da privacidade; os dados pessoais. Se a privacidade é contextual, a proteção de dados é objetiva, com dados e informações pessoais concretas, cuja coleta incide no exercício da própria cidadania. Estas informações são cada vez mais utilizadas para a construção de perfis e categorizações que, muitas vezes, servem para discriminar pessoas a partir de critérios muito pouco transparentes, aumentando assim as desigualdades sociais (O'Neil, 2016). Conforme discutido estas informações são individuais, mas ao serem agregadas tornam-se objeto de uma regulação coletiva. Isto ocorre devido ao fato do modelo de negócios das grandes empresas de tecnologia estar calcado na essência cibernética da tecnologia digital; a informação. De fato;

> Ainda que registros computadorizados de informações pessoais estejam no centro de muitas empresas, a marca distintiva deste setor é que a informação é sua empresa, sua moeda e seu modelo comercial. Instituições financeiras, empresas de cartões de crédito, companhias de seguros e hospitais, por exemplo, mantêm sistemas de registro maciços, mas o fazem com outro objetivo que é sua missão principal. Não é assim para os provedores de serviços de informação. Sua razão de ser é a informação. (Nissenbaum, 2009, p. 45)

É neste contexto em que se discute qual o papel dos Estados em regular este mercado a fim de garantir direitos e liberdades. Os modelos regulatórios adotados por países do norte global, considerados democracias liberais consolidadas, refletem valores sociais e éticos intrínsecos ao próprio sistema democrático. Visões sobre direitos humanos, o exercício da liberdade de expressão e da cidadania, e a própria participação política manifestam-se nas abordagens normativa destes países.

Regular não significa restringir, ou dificultar o surgimento de inovações tecnológicas. Significa traçar diretrizes e parâmetros para que determinado setor atue com transparência para com a sociedade e de forma compatível com a democracia e o Estado de direito. Todos os setores da economia são objeto de algum nível de regulação e o mercado de tecnologia não pode ser exceção, pois conforme discutido a ausência de normas claras sobre o uso de dados pessoais gerou o fenômeno do capitalismo de vigilância. Suas consequências para as democracias contemporâneas apenas

começam a ser observadas e desde já o diagnóstico indica que é necessário regular a atuação destas empresas.

O capítulo está dividido em três partes. Inicia-se resgatando o histórico do debate sobre proteção de dados a partir da perspectiva da União Europeia, para analisar em seguida o Regulamento Geral sobre a Proteção de Dados, em vigor desde 26 de maio de 2018. Ao avaliar aspectos normativos da proteção de dados pessoais, busca-se identificar questões que impactam as democracias contemporâneas, o exercício da cidadania e dos direitos e das liberdades. Para tanto, realiza-se uma análise crítica e descritiva dos principais aspectos do regulamento, que inspirou outras normas jurídicas ao redor do mundo, inclusive a lei brasileira de proteção de dados pessoais. Serão descritos os principais conceitos e princípios de proteção de dados pessoais. Em seguida, destaca-se os direitos consolidados com a norma europeia, como por exemplo, a controvérsia sobre a retirada de conteúdo na Internet. Apresenta-se as obrigações e responsabilidades dos agentes de tratamento de dados, sejam eles da iniciativa privada, ou dos próprios Estados membro da União Europeia. Por fim, destaca-se os mecanismos de responsabilização destes agentes e possíveis sanções aplicadas em caso de violação da legislação.

Na segunda parte do capítulo o foco passa a ser o modelo regulatório dos Estados Unidos, onde se encontram as grandes corporações de tecnologia. Marcado por uma diversidade de leis, que variam inclusive de acordo com a região do país, observa-se que se trata de uma legislação com ênfase nos direitos dos consumidores. Além disso, foi fortemente influenciada pelos ataques de 11 de setembro de 2001, em Nova Iorque. Este acontecimento levou à suspensão de regulamentos sobre proteção de dados pessoais e privacidade em nome do combate ao terrorismo. Alicerçada em um modelo extremamente neoliberal, a abordagem estadunidense se caracteriza pela auto regulação do mercado, ou seja, a ausência do Estado na mediação entre os direitos dos cidadãos/consumidores e das empresas. Enfatiza-se a *California Consumer Privacy Act* (CCPA), legislação regional, considerada um reflexo do regulamento europeu, que entrou em vigor em janeiro de 2020. Por fim, discute-se questões relacionadas ao direito à concorrência, conhecido como leis *antitruste*, que são legislações que buscam regular o setor privado, proteger os consumidores, restringir a formação de cartéis, dentre outras medidas, para promover o livre comércio.

Na terceira parte, explora-se a lei brasileira de proteção de dados e suas principais características. Inicia-se resgatando seu histórico a partir do debate em torno do Marco Civil da Internet e a tramitação dos projetos de lei sobre proteção de dados pessoais no Congresso Nacional. São destacadas as alterações realizadas na lei, com destaque para a vinculação da Autoridade Nacional de Proteção de dados pessoais à presidência da República e a retirada do direito de revisão humana

após decisão automatizada. São discutidas ainda a criação do Cadastro Base do Cidadão[27], que irá reunir mais de cinquenta bancos de dados com informações pessoais e suas incompatibilidades com a própria lei geral de proteção de dados. Por fim, são comparados os principais aspectos da lei brasileira com os modelos regulatórios da União Europeia e dos Estados Unidos.

2.1 – Regulamento Geral sobre a Proteção de Dados da União Europeia

O debate sobre proteção de dados pessoais na União Europeia tem como marco histórico a Convenção de Estrasburgo, conhecida como Convenção 108, do Conselho da Europa, embrião da União Europeia. A Convenção, ocorrida em 1981, teve como tema a "Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal[28]". É o primeiro ordenamento jurídico internacional que dispõe expressamente sobre proteção de dados. O direto à privacidade já estava presente na declaração Universal dos Direitos do Homem, desde 1948.

A convenção alicerça a preocupação do Conselho da Europa sobre a expansão das tecnologias da informação e comunicação e seus impactos na sociedade, mesmo antes da consolidação de fenômenos como a *big data, machine learning,* Internet das coisas, ou cidades inteligentes. O documento dispõe sobre o tratamento de dados pessoais realizado tanto pelo setor privado como pelos governos, inclusive autoridades policiais e judiciárias. Demonstra a preocupação com o tratamento de dados pessoais de forma automatizada e as consequências de escolhas e decisões tomadas por máquinas para a sociedade. Como resultado, paulatinamente, os Estados membros do Conselho da Europa adotam leis de proteção de dados pessoais e comprometem-se a respeitar as diretrizes de tratamentos de dados, em especial no que se refere aos direitos e liberdades fundamentais de seus cidadãos.

Em 1995, o Parlamento Europeu e o Conselho da União Europeia publicam uma diretiva[29] "relativa à proteção dos indivíduos no que diz respeito ao tratamento de dados pessoais e ao livre movimento de tais dados". O documento apresenta definições de termos que continuam atuais tais como; dados pessoais e processamento de dados pessoais, apontando inclusive a necessidade do consentimento na coleta de dados. Ao final da norma, observa-se a solicitação de que todos os Estados membros da União Europeia tomem providências para aplicar a diretiva por meio de leis locais, entrando em conformidade com a regulação do bloco.

---

[27] Sobre os decretos 10.046 e 10.047. Disponível em https://theintercept.com/2019/10/15/governo-ferramenta-vigilancia/?fbclid=IwAR3rCoD-COM1V73pPdq2UeAXTHkNY_F4wuesoT4DESgXuJzRmsEB5qxnoNc. Acesso em 23/9/19.

[28] Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Disponível em < https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm >. Acessado em 7/2/19.

[29] Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN. Acessado em 7/2/19.

A proteção de dados pessoais torna-se um direito fundamental na Carta de Direitos Fundamentais da União Europeia, de 2000[30]. Outra importante diretiva publicada, em 2008, pelo Conselho da União Europeia é "relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matérias criminais"[31]. O documento tem como um de seus objetivos proteger os direitos e liberdades fundamentais, em particular o direito à privacidade, "quando para efeitos de prevenção, investigação, detenção ou repressão de infrações penais, ou execução de sanções penais, os dados pessoais são transmitidos entre as autoridades dos Estados membros do bloco[32]". Observa-se nesta diretiva a presença de uma preocupação distinta, com foco na prevenção do vazamento de informações entre fronteiras e uma regulação da atuação policial e judicial, no que se refere ao tratamento de dados pessoais. A norma atua em duas grandes frentes. Primeiramente, determina um modelo de atuação destes agentes que busca a eficiência, ao mesmo tempo que previne o abuso destas autoridades no tratamento de dados pessoais. Em seguida, estabelece um conjunto de melhores práticas, que leva em consideração a privacidade, a proteção de dados nas investigações criminais, demonstrando preocupação com os direitos individuais e uso inapropriado de dados por parte destas autoridades.

No ano seguinte, em 2009, com o Tratado de Lisboa[33], o direto à proteção de dados pessoais se torna um direito fundamental no âmbito da União Europeia. Mas é em 2012, que o Comitê Europeu de Proteção de Dados propõe a reforma das regras de 1995, com o objetivo de aumentar o controle das pessoas sobre os próprios dados e diminuir a burocracia envolvida em seu tratamento, realizado por agentes públicos, ou privados. O resultado desta reforma, que inclui também uma revisão da diretiva de dados pessoais no âmbito das investigações policiais e judiciais, é o Regulamento Geral sobre a Proteção de Dados, finalizado em 27 de abril de 2016[34].

As principais transformações da reforma são o estabelecimento de uma série de regras sobre proteção de dados que removem alguns requerimentos administrativos com o objetivo de diminuir a burocracia e desonerar o setor empresarial e o governamental. Na prática, o impacto foi que ao invés de notificar as autoridades de proteção de dados sobre todas as práticas de processamento de

---

[30] carta de direitos fundamentais da união europeia. Disponível em <https://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em 3/3/20.

[31] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0977&from=EN>. Acessado em 7/2/19.

[32] *Ibdem*.

[33] Tratado de Lisboa. Disponível em < http://www.europarl.europa.eu/about-parliament/pt/powers-and-procedures/the-lisbon-treaty >. Acessado em 7/2/19.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> Acessado em 7/2/19.

informações, as novas regras criam mecanismos de responsabilização e prestação de contas para aqueles que trabalham com o tratamento de informações pessoais.

O consentimento, que já estava presente no documento de 1995, deixa de ser presumido e passa a ter a necessidade de ser explícito, ou seja, todos aqueles que trabalham com o processamento de dados pessoais precisam perguntar sobre o uso dos dados antes de sua coleta e tratamento. A regulação garante ainda uma série de direitos para os titulares dos dados, as pessoas físicas. Cria mecanismos de conformidade e responsabilização para empresas e governos, além de prever sanções e multas administrativas.

Por fim, a nova norma é válida para todos os cidadãos europeus, mas se aplica a todas empresas e governos que atuam na região, impactando globalmente o setor de tecnologia. A regulação também se aplica a pessoas jurídicas, ampliando as regras para profissionais liberais, pequenas empresas, ou toda e qualquer profissão que colete dados pessoais. Na prática isto significa que, além de governos e empresas de tecnologia, farmácias, dentistas, advogados, universidades e todo e qualquer setor que colete informações pessoais, como números de documentos, data de nascimento, dentre outros, precisam se adaptar às novas regras, ou estarão sujeitos a multas e a eventuais processos judiciais.

Sobretudo, a principal diferença entre estes três documentos é de caráter jurídico. As diretivas, tanto a de 1995, quanto a de 2008, são documentos que buscam traçar diretrizes comuns no âmbito da União Europeia. Já o regulamento vincula a obrigatoriedade a todos países que pertencem ao bloco, além de se tratar de uma legislação diretamente aplicável. Portanto, se os primeiros documentos possuíam um caráter sugestivo – já que cada país poderia incorporar à sua maneira as diretrizes – a partir de maio de 2018 todos Estados membro da União Europeia são obrigados a cumprir o Regulamento Geral sobre a Proteção de Dados.

Após esta contextualização histórica, parte-se para a análise do documento. O Regulamento Geral sobre a Proteção de Dados parte de premissas – ou seja, decisões e acórdãos anteriores no âmbito da União Europeia – dentre os quais o primeiro deles é que "a proteção de pessoas naturais em relação ao processamento de dados pessoais é um direito fundamental[35]".

O escopo material do regulamento é o processamento de dados pessoais, seja ele feito por meio de formulários físicos ou *online*, processados manualmente, ou de forma automatizada, com exceção de; atividades que fogem do escopo das leis da União Europeia, questões de segurança nacional e que correm em segredo de justiça, atividades como cooperação política, prevenção de conflitos, ajuda humanitária, e atividades domésticas (como correspondência e uso de redes sociais).

O 4º artigo descreve vinte e seis definições da regulação, englobando questões sobre os dados

[35] *Ibdem*.

em si, seu processamento e tratamento, os atores envolvidos em seu tratamento, dentre outras definições fundamentais para compreender seu escopo. Como é um documento técnico, com termos que podem causar confusão, a seguir destaca-se os conceitos mais relevantes para sua compreensão. Optou-se por agrupá-los não na ordem em que são descritos, mas de forma conceitual; ou seja, definições de dados; de tratamento de dados e de atores envolvidos no tratamento de dados.

2.1.1 – Principais definições

O regulamento indica como definição de dado pessoal "toda informação relativa a uma pessoa singular identificada, ou identificável[36]", conhecida como titular dos dados, ou sujeito de dados. O documento ainda destaca tipos de dados pessoais, tais como; dados genéticos, dados biométricos e dados relativos à saúde. É importante ressaltar que esses dados pessoais são informações que se configuram em diferentes formatos, tais como; alfabético, numérico, gráfico, fotográfico, acústico, dentre outros que são armazenados de forma analógica, ou digital.

Dentre as categorias de dados há aqueles considerados especiais, ou sensíveis, que englobam informações pessoais que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas, ou filosóficas, a filiação sindical, os dados genéticos e dados biométricos, dados relativos à saúde, ou dados relativos à vida sexual, ou orientação sexual de uma pessoa. Englobam, portanto, informações comportamentais e biológicas. O tratamento destes dados é proibido a não ser que a pessoa forneça o consentimento explícito.

Outra importante definição do regulamento é o conceito de consentimento do titular dos dados. O entendimento é de que se trata "da manifestação de vontade, livre, específica, informada e explícita, pela qual o titular aceita, mediante declaração, ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam tratados[37]". O consentimento explicito é um dos grandes avanços da regulação, pois impacta diretamente no formato dos termos de uso dos programas e aplicativos digitais. Estes documentos, que em geral se assemelham a bulas de remédio, ou seja, longos e com muitos itens, ao menos na teoria teriam que se tornar mais simples e fáceis de ler, para de fato incorporarem a noção de consentimento explicito da coleta de dados.

O artigo 4º também indica o que é a limitação do tratamento de dados; "a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro[38]". Estas limitações são aplicadas, em especial, aos dados pessoais ou sensíveis. A limitação é um instrumento preventivo, que busca reduzir as formas com que uma informação pode ser associada a determinada

[36] *Ibdem.*
[37] *Ibdem*
[38] *Ibdem*

pessoa de forma a identificá-la.

Por fim, é considerada uma violação de dados pessoais, "um atentado de segurança que provoque, de modo acidental, ou ilícito, a destruição, a perda, a alteração, a divulgação, ou o acesso, não autorizados, a dados pessoais transmitidos, conservados, ou sujeitos a qualquer outro tipo de tratamento[39]". Ou seja, qualquer tipo de vazamento de informações, seja ela acidental, ou proposital – como invasões, por exemplo – é considerada uma violação do direito dos titulares de dados.

Esta são as principais definições envolvendo os dados. A seguir reproduz-se outra importante conceituação que se refere ao tratamento de dados;

> Uma operação, ou um conjunto de operações efetuadas sobre dados pessoais, ou sobre conjuntos de dados pessoais, por meios automatizados, ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação, ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão, ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição[40].

Importante observar que o regulamento já parte da premissa de que os dados são coletados e busca atuar na etapa seguinte que é justamente o que é conhecido como jargão do setor como mineração de dados. A definição de tratamento, portanto, engloba todas as etapas de seu processamento, ou seja, todo o ciclo de vida dos dados, do momento em que são gerados até sua eventual destruição. No âmbito do tratamento de dados, o regulamento define duas importantes práticas realizadas pelo setor; a definição de perfis, conhecido pelo termo inglês *profiling* e a anonimização de dados. A primeira delas é definida como;

> Qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar, ou prever aspetos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização, ou deslocações[41].

A prática de construção de perfis de forma automatizada é um dos aspectos que geram mais controvérsias sobre os possíveis impactos na sociedade quando o tema é a proteção de dados pessoais. O conjunto de técnicas para a criação de perfis -inclusive com dados biométricos e reconhecimento facial – já é amplamente utilizado em diversos setores, que vão de instituições financeiras à planos de saúde, passando pelo varejo, entretenimento e até mesmo pelos órgãos policiais e jurídicos. Portanto, esta prática é uma das que mais influenciam o exercício da cidadania e dos direitos e liberdades fundamentais, já que as pessoas são agrupadas de acordo com determinadas características,

---

[39] *Ibdem*.
[40] *Ibdem*
[41] *Ibdem*

que não necessariamente são fixas. Além disso, a construção de perfis tende a reproduzir padrões de discriminação e categorias que aprofundam as desigualdades, ao privilegiar determinados dados em detrimento de outros. Somado a todos estes fatores não há transparência sobre como operam. A construção de perfis se torna ainda mais problemática quando é realizada de forma automatizada, ou seja, por meio de algoritmos capazes de tomar decisões que influenciam a vida das pessoas. Por todos estes motivos a prática de construção de perfis é condenada e no contexto do Regulamento Geral sobre a Proteção de Dados e só poderá ser realizado mediante o consentimento explícito.

Para contrabalancear esta prática, muitas instituições – governos e corporações – se respaldam na anonimização, ou pseudoanonimização, durante o tratamento de dados. Estas técnicas fazem com que determinadas informações, especialmente as consideradas sensíveis, sejam mantidas separadamente, tornando sua relação com outros dados independente. Ambas se referem a aplicação da limitação no tratamento dos dados. Já a pseudoanonimização ocorre quando alguns dados são separados ou ocultos de outros. Por sua vez, a anonimização seria tornar a identificação do titular de dados virtualmente impossível. Esta técnica mantêm os dados sensíveis, mas exclui do tratamento toda e qualquer informação que possa relacionar aqueles dados à pessoa.

Esta são as principais definições relativas a dados pessoais, suas subcategorias, como os dados sensíveis e as conceituações em torno do tratamento de dados e práticas específicas realizadas após a coleta das informações. A seguir, destaca-se a definição dos principais atores envolvidos no tratamento de dados, além do titular de dados, já mencionado.

Há uma pluralidade de atores que trabalham com o tratamento de dados pessoais e cada um deles tem obrigações e responsabilidades específicas, descritas mais adiante neste capítulo. Por se tratar de termos técnicos destaca-se abaixo um quadro com o nome em inglês, português de Portugal (que é a tradução oficial da União Europeia) e como o termo é conhecido no Brasil, seguido de sua definição[42].

[42] *Ibdem*

Quadro 1: Atores envolvidos no tratamento de dados pessoais da União Europeia.

Ator (inglês)	**Ator (pt)**	**Ator (pt_br)**	**Definição**
Data controller	Responsável pelo tratamento	Controlador de dados	a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais;
Data processor	Subcontratante ou Processador	Operador	uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;
Recipient	Destinatário	Receptor	uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro.
third party	Terceiro	Terceiro	a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;
Supervisory authorities	Autoridade de controlo	Autoridade Nacional de Proteção de Dados	uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51.
Fonte: Regulamento Geral sobre Proteção de Dados da União Europeia.			

Os atores que trabalham com o tratamento de dados pessoais podem ser classificados em dois conjuntos distintos; o Estado e suas autoridades reguladoras e o setor privado, sujeito às obrigações e responsabilidades determinadas pela norma e passíveis de sanções em caso de violação. Sendo assim, os controladores, operadores, receptores e terceiros são os agentes que trabalham com o tratamento de dados pessoais, que são fiscalizados por uma, ou mais autoridades de proteção de dados.

Em primeiro lugar, ressalta-se que os controladores, ou responsáveis pelo tratamento, são aqueles que determinam os propósitos e meios de processar dados pessoais. Estes controladores podem atuar individualmente, ou de forma conjunta, quando se tornam controladores conjuntos.

Já os operadores, ou subcontratantes, são aqueles envolvidos no processamento de dados pessoais em nome dos controladores, assim como os receptores e terceiros. Para diferenciá-los é necessário identificar as finalidades e meios de processar os dados, ou seja, quais dados são coletados e por qual motivo? Por que determinados dados são coletados e o que será feito com eles? O ator que define isso é o responsável pelo tratamento, ou controlador, e os que o auxiliam a realizar esta atividade são os operadores, recipientes ou terceiros.

Portanto, os responsáveis pelo tratamento, ou controladores, possuem mais responsabilidades e obrigações do que os operadores, recipientes e terceiros. Eles podem ser pessoas físicas, como médicos, jornalistas, advogados e outras pessoas que processam informações sobre indivíduos. Podem ser também pessoas jurídicas, como empresas, instituições educacionais, governos, organizações sem fins lucrativos, entre outras. No caso de violação de dados é importante identificar o controlador, ou seja, quem coletou os dados inicialmente, por qual meio e para qual finalidade.

Os operadores, ou subcontratantes, são aqueles que tratam os dados em nome dos controladores, e não possuem o poder de decisão sobre como realizar esta atividade, já que trabalham a partir das instruções dos responsáveis pelo tratamento. Os recipientes e terceiros, que são contratados pelo controlador, seguem as mesmas regras.

Todos estes atores que tratam dados pessoais precisam contar com um agente de proteção de dados, ou encarregado da proteção de dados na tradução oficial, ou no original *Data Protection Officers*, DPO. Estes agentes são responsáveis por informar e orientar as empresas, instituições, pequenos negócios, pessoas físicas e governos sobre as práticas necessárias para cumprir com o regulamento. Podem ser contratados diretamente, ou terceirizados, ou seja, pessoas físicas ou jurídicas. O encarregado pode representar mais de um órgão público ou empresa, de acordo com sua capacidade e estrutura, desde que tenha conhecimento sobre as obrigações e responsabilidades dos operadores, controladores, recipientes ou terceiros.

A atuação destes profissionais ou empresas é orientada pelo Comitê Europeu para a Proteção de Dados, responsável pela elaboração de códigos de conduta e certificações dos encarregados de proteção de dados. O Comitê é um órgão independente da União Europeia que possui uma série de outras atribuições, como emitir pareceres e diretrizes, sendo composto por um presidente e um representante de cada um dos países membros da União Europeia. Esta autoridade tem ainda a função de coordenar a atuação das autoridades nacionais, sendo responsável por lidar com a transferências de dados entre fronteiras. Desde as primeiras diretivas da década de 1990, a União Europeia proíbe a transferência de dados para países que não cumprem com as mesmas exigências de privacidade e proteção de dados.

Por fim, é importante destacar o papel da autoridade de dados, definida no 4º artigo do regulamento e aprofundada no quinto capítulo do documento. A regulação determina que cada país tenha uma autoridade de controle independente do governo, responsável pela fiscalização, aplicação das regras e pela defesa dos direitos dos titulares de dados, inclusive com poderes de investigação. O regulamento é assertivo em destacar a independência da autoridade, inclusive financeira. A autoridade pode ser uma única agência, ou autarquia, ou um conjunto de instituições, como funcionam a rede de proteção aos consumidores no Brasil (Procons). Cada Estado membro tem autonomia para definir seu arranjo nacional, mas independente do modelo adotado, a autoridade nacional é responsável pela

aplicação do Regulamento Geral sobre a Proteção de Dados em cada um dos países do bloco.

O papel destes atores será aprofundado nas seções sobre obrigações e responsabilidades, assim como na de sanções e mecanismos de conformidade dos agentes. Antes de prosseguir é importante destacar os princípios norteadores do Regulamento Geral sobre a Proteção de Dados.

2.1.2 – Princípios de proteção de dados

Os princípios de proteção de dados orientam a atuação dos controladores e operados, sejam eles do setor privado, ou do próprio governo. São conceitos que buscam alicerçar os direitos garantidos pela norma. Há seis princípios descritos no artigo 5º da regulação. Além deles, uma das condições para o tratamento de dados é o consentimento explicito do titular de dados. Por fim, em seu artigo 25º descreve a necessidade de se adotar a proteção de dados desde a concepção e por padrão (*privacy by design*).

O primeiro princípio estabelece que os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados. Este princípio garante que os titulares dos dados saibam com qual objetivo seus dados são tratados e quais são as organizações responsáveis. A transparência é um aspecto fundamental para garantir que os dados pessoais não sejam compartilhados com terceiros sem que haja o consentimento explícito do titular de dados.

O segundo princípio existe para garantir que os dados sejam coletados para fins específicos e não genéricos, mas a regulação permite que informações sejam agregadas para fins estatísticos, pesquisas científicas, históricas e interesse público, desonerando assim, instituições de pesquisa, universidades e governos. A limitação da finalidade restringe a coleta e tratamento de dados de forma indiscriminada, em especial os dados sensíveis. Por exemplo, para obter um serviço de e-mail é necessário informar o gênero com que uma pessoa se identifica? Para utilizar um aplicativo de hospedagem a raça é um quesito indispensável? Ou a solicitação destas informações sensíveis servem para orientar a construção de perfis? Este princípio busca explicitar a relação entre os dados coletados e o serviço oferecido, ressaltando a necessidade efetiva da coleta de dados. As pessoas podem consentir explicitamente em fornecer tais informações, mas ao estabelecer a limitação das finalidades enquanto um princípio, a regulação busca minimizar a coleta indiscriminada de informações, o que leva ao próximo conceito.

O terceiro princípio de minimizar os dados é similar ao segundo, pois reforça que sejam coletados apenas os dados necessários, com finalidade específica. Sua diferença é ressaltar que não sejam coletadas informações consideradas estritamente necessárias para o processamento proposto pelo responsável pelo tratamento das informações. Em teoria, este princípio excluiria informações

consideradas irrelevantes para determinados serviços, como nos exemplos acima citados. Afinal de contas, raça, orientação sexual, religião, dentre outras informações são considerados dados sensíveis e sua coleta só pode ser realizada mediante o consentimento explícito do titular de dados.

A exatidão, o quarto princípio da proteção de dados, se refere à necessidade de que os dados sejam atualizados quando necessário. As informações desatualizadas devem ser apagadas, ou retificadas o quanto antes. Este princípio reforça alguns direitos que serão abordados na próxima seção, como por exemplo o direito de remoção de conteúdo. Qual a real necessidade de um controlador ter em seu banco de dados todos os endereços de um determinado indivíduo nos últimos 10 anos? Novamente, observa-se que os princípios do Regulamento Geral sobre a Proteção de Dados buscam atuar na redução do impacto da construção de perfis.

Nesta mesma linha, o quinto princípio de limitação da conservação dos dados impõe que os controladores guardem os dados pessoais apenas pelo tempo necessário para realizar o tratamento específico, indicando que a reutilização de dados pessoais não é uma prática aceitável (ainda que amplamente realizada, inclusive comercializada). A regulação abre a exceção para o armazenamento de dados por longos períodos apenas para fins estatísticos, pesquisas científicas, históricas e interesse público.

Por fim, o último princípio da integridade e confidencialidade busca garantir a segurança dos dados coletados e tratados, protegendo o tratamento de dados por terceiros não autorizados, sua utilização ilegal, eventuais danos, ou perda de dados. Medidas de segurança tais como criptografia, mecanismos de autenticação e autorização, são utilizadas para garantir a segurança dos dados. A regulação reforça que o controlador está sujeito à responsabilização (*accountability*) caso qualquer um dos princípios seja violado. As sanções impostas pela regulação serão discutidas posteriormente.

Antes de prosseguir é necessário abordar outros dois importantes aspectos da regulação referentes ao consentimento e a privacidade por padrão (*privacy by design*). Ao colocar o consentimento explícito como condição para o tratamento dos dados a regulação busca, por um lado, conscientizar as pessoas de que seus dados são utilizados e, por outro, ampliar a margem de negociação com as grandes empresas de tecnologia.

Outra frente que o consentimento explícito busca combater é a prometida "experiência de uso" das pessoas, razão pela qual as empresas alegam que os dados pessoais são coletados de forma indiscriminada. Ao determinar que o consentimento deve ser específico, informado e não ambíguo, a regulação enfatiza a necessidade da alteração dos termos de uso para modelos mais diretos e objetivos, tornando indispensável que o consentimento seja dado por meio de uma declaração, ou ação afirmativa. Por fim, a suspensão do consentimento pelo titular de dados deve ser informada e pode ser realizada a qualquer momento.

Toda esta necessidade de informar às pessoas sobre o que é coletado e tratado é vista de forma

diferenciada para menores de idade, já que a regulação compreende que este grupo de pessoas não é tão bem informado sobre seus direitos. Em seu artigo 8º determina que o consentimento de menores de dezesseis anos só será considerado lícito se for dado por um responsável do menor. Os Estados membros do bloco podem criar leis nacionais para diminuir a idade dos considerados menores, desde que ela não seja inferior a treze anos.

Outra fundamental transformação proposta pela regulação é a privacidade por padrão (Cavoukian, 2011). Em um universo em que os aplicativos, sistemas e dispositivos são projetados para coletar o máximo de informação possível, a privacidade por padrão é uma mudança bastante radical. Este conceito destaca que o direto à privacidade e a proteção de dados pessoais não deve se limitar às medidas regulatórias e normalizações jurídicas. Organizações que processam dados pessoais, devem adotar princípios da privacidade por padrão desde a concepção de seus produtos e sistemas. Cavoukian (2011), responsável por cunhar o conceito, destaca elementos fundamentais para a abordagem da privacidade por padrão.

Primeiramente, alerta para o fato de que os aplicativos e sistemas sejam voltados para a necessidade das pessoas – conhecido do termo em inglês de *user centered design, ou* design centrado no usuário - e que a segurança é uma parte integral deles, presente durante todo o ciclo de vida dos produtos, programas ou aplicativos (Preece *et all*, 2005). Com isto, ressalta que a visibilidade e a transparência são essenciais para que os sistemas sejam funcionais. Estes princípios são descritos no 25º artigo da regulação, que por sua vez destaca que as organizações devem tomar as medidas necessárias para proteger a privacidade das pessoas considerando; o estado da arte dos sistemas, os custos para sua implementação, a natureza, o escopo, o contexto e as finalidades de processamento, e por fim, os riscos envolvidos em violar direitos e liberdades.

Por fim, os princípios do Regulamento Geral sobre a Proteção de Dados devem nortear a atuação tanto dos controladores, como dos operadores sejam eles pessoas físicas, o setor privado e o próprio Estado. Observa-se que os princípios orientam a atuação dos agentes que tratam dados pessoais, além de indicar alguns direitos dos titulares de dados, aprofundados a seguir.

2.1.3 – Direitos dos titulares de dados

O terceiro capítulo do Regulamento Geral sobre a Proteção de Dados é composto por onze artigos que descrevem os direitos dos titulares dos dados. Em primeiro lugar, estabelece a transparência e regras para o exercício dos direitos dos titulares dos dados. A transparência, como observado na seção anterior, é um princípio da regulação que determina que as pessoas sejam informadas de todo tratamento de seus dados, por quem e por qual motivo. As regras determinam como isto deve ser feito; por meio do consentimento explícito realizado de forma consciente a partir

de contratos claros, inteligíveis e objetivos.

Partindo destas premissas, o titular de dados tem o direito de solicitar e adquirir acesso aos seus dados pessoais a qualquer momento. Ou seja, pode obter dos controladores uma confirmação sobre quais dados são coletados e para qual finalidade, além de receber uma cópia de todos os dados coletados desde sempre.

A consolidação deste direito tem como base um processo judicial aberto pelo austríaco Max Schrems, em 2011, contra grandes corporações de tecnologia. Por meio da ONG Europe x Facebook[43], ele denunciou ao Conselho de Proteção de Dados Irlandês, onde a empresa mantém sua filial europeia, o tratamento indevido dos dados. Ao solicitar as informações pessoais coletadas pela plataforma, ele recebeu um documento com mais de mil e duzentas páginas em que descobriu, dentre outras coisas, que até as mensagens apagadas eram gravadas em uma categoria intitulada "*deleted*".

Na ação Schrems conseguiu demonstrar que o Facebook não respeitava seu direito à privacidade previsto na Carta dos Direitos Fundamentais da União Europeia, já que suas informações pessoais eram transferidas para os Estados Unidos, o que rompia o acordo conhecido como *Safe Harbour* ("porto seguro"). Desde as diretivas da década de 1990, a União Europeia determina que os dados de seus cidadãos só sejam transferidos para fora do bloco para países que possuem as mesmas diretrizes de privacidade e proteção de dados pessoais. Por isso, em 2015 o Tribunal de Justiça da União Europeia invalidou o acordo entre o bloco e os Estados Unidos para a transferência entre fronteiras de dados pessoais, abrindo precedentes para a implementação do RGPD.

Em 2018, Schrems fundou a organização sem fins lucrativos *None of Your Business* (NOYB)[44], com o objetivo de defender os direitos dos titulares previstos na legislação. Uma de suas primeiras iniciativas[45] foi uma ação contra o Google e o Facebook alegando que as empresas agem de forma coercitiva para que as pessoas aceitem os termos de uso de suas plataformas. Na ação, em que as empresas podem ser multadas em quase quatro bilhões de euros, Schrems questiona justamente a ausência do consentimento explícito e esclarecido determinado pela norma.

Além do direito ao acesso aos dados pessoais, a legislação garante que as pessoas possam contestar e/ou restringir a coleta e tratamento de seus dados. Este direito é exercido quando o titular de dados não quer que suas informações componham bancos de dados de perfis (*profiling*), ou de marketing direcionado. Além disso, os titulares de dados podem solicitar a retirada de informações quando os propósitos da coleta já não mais se justificam, ou são relevantes, com exceção para informações de interesse público.

---

[43] Europe x Facebook. Disponível em < http://europe-v-facebook.org/ >. Acesso em 23/9/19.
[44] Non of your business. Disponível em < https://noyb.eu/>. Acesso em 23/9/19.
[45] Max Schrems files first cases under GDPR against Facebook and Google. Disponível em < https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177 >. Acessado em 7/2/19.

Semelhante ao direito de restringir o tratamento de dados, o direito a oposição permite com que qualquer pessoa solicite aos controladores que seus dados deixem de ser tradados, em especial para efeitos de comercialização direta e construção de perfis. Este direito de oposição ao tratamento de informações pessoais impacta não apenas no marketing direcionado como na indústria do spam, já que ao menos em teoria, basta solicitar a retirada dos dados pessoais de determinado banco de dados uma única vez, sem necessidade de justificativa.

A principal diferença entre o direito de restrição e o de oposição é que no primeiro caso os controladores continuam coletando alguns dados, mas no segundo a cessão deve ser imediata. As exceções novamente envolvem interesse público, pesquisas científicas, históricas e fins estatísticos. A regulação também prevê o exercício do direito de reparação, que ocorre quando o titular dos dados requer que suas informações sejam retificadas, em caso de inconsistências, como por exemplo, a grafia de um sobrenome errado em determinado banco de dados.

Um dos direitos mais controversos garantido pelo Regulamento Geral sobre a Proteção de Dados é o direito de solicitar a remoção, ou apagamento de determinado conteúdo. Sua base jurídica já estava presente na diretiva de 1995, já que o direito à remoção de dados está implícito no direito ao controle dos próprios dados. Entretanto a questão ganhou destaque nos debates sobre o "direito ao esquecimento" a partir de um caso ocorrido originalmente na Espanha, em 2009. A controvérsia envolveu a digitalização e inserção na web de uma publicação de 1998, do jornal espanhol *La Vanguardia*, em que apareciam nomes de proprietários de imóveis cujos bens seriam vendidos para quitar dívidas previdenciárias. Um deles, Mario Costeja González, entrou em contato com o jornal solicitando a retirada de seu nome, alegando que a transação havia ocorrido há anos, mas seu nome continuava aparecendo nos resultados de busca do Google. O jornal se recusou a retirar a publicação o que levou González a acionar diretamente o Google por meio da Agência Espanhola de Proteção de Dados.

Em 2014, o Tribunal de Justiça da União Europeia decidiu que mecanismos de busca na Internet são responsáveis pelo processamento de informações pessoais que aparecem em páginas de terceiros[46]. A decisão abriu precedentes para a remoção de conteúdo em casos específicos, como por exemplo, fatos irrelevantes, ocorridos há muito tempo, ou considerados inadequados. O caso ficou conhecido como o direito ao esquecimento, entretanto o termo esquecimento não é o mais adequado para descrevê-lo. Diz respeito muito mais à desindexação dos mecanismos de busca do que seu apagamento, ou remoção de determinado conteúdo da Internet.

Um dos aspectos mais relevantes deste debate é com relação à responsabilização dos

[46] Justiça europeia decide que Google é obrigada a apagar links de buscas a pedido de internautas. Disponível em < https://oglobo.globo.com/economia/justica-europeia-decide-que-google-obrigada-apagar-links-de-buscas-pedido-de-internautas-12468545 >. Acessado em 7/2/19.

mecanismos de busca, encarregados de indexar e organizar conteúdo na Internet, mas não necessariamente os controladores originais, ou os primeiros publicadores do conteúdo. No Brasil e nos Estados Unidos o entendimento é diferente. Nestes ordenamentos apenas a publicação original é responsabilizada, eximindo os intermediários dos deveres associados a práticas como disseminação de conteúdo falso, discurso de ódio, dentre outras práticas. Nos Estados Unidos esta norma tem origem no *Communications Decency Act*, de 1996, portanto, anterior à indexação da web. Já no Brasil, a regulação está no Marco Civil da Internet, de 2014. O tema será retomado adiante, mas é importante enfatizar que esta controvérsia está no centro do que Zuboff (2019) caracteriza como indiferença radical das companhias de tecnologia da atualidade.

Por outro lado, o Regulamento Geral sobre a Proteção de Dados prevê algumas exceções ao direito de remoção de conteúdo. A solicitações devem considerar o exercício do direito à liberdade de expressão e de informação, e quando o arquivo for de interesse público, de saúde pública, pesquisa científica, ou para fins estatísticos. Portanto, não se trata de um direito ao esquecimento, como ficou conhecido inicialmente, mas o direito de solicitar a remoção de um dado pessoal específico e de forma justificada. Longe de esgotar a controvérsia sobre a remoção de conteúdo na Internet, ressalta-se que o debate deve envolver não apenas o autor original da publicação como também os meios pelos quais o conteúdo circula, ou seja, as plataformas de conteúdo que operam como intermediários ou *gatekeepers*.

Ponderadas estas questões, destaca-se que outro importante direito garantido que é o da portabilidade dos dados (Fialová, 2014). Decorrente da possibilidade de acesso, o titular dos dados pode solicitar que suas informações sejam disponibilizadas pelos controladores em um formato estruturado, legível por máquina e comumente utilizado, semelhante ao formato de dados abertos. Na prática o exercício de deste direito possibilita que um titular de dados tenha suas informações pessoais e as ceda entre um ou outro controlador da forma que determinar.

Por fim, o 22º artigo da regulação aborda a questão de decisões individuais automatizadas, incluindo definição de perfis, ou seja, processos decisórios em que os algoritmos definem as categorias dos dados pessoais. A regulação estabelece o direito de cada pessoa não estar sujeita à uma decisão tomada por processos automáticos. As pessoas só estarão sujeitas a tomadas de decisões automáticas caso forneçam consentimento explícito, ou celebrem um contrato específico com os controladores para esta finalidade. Este direito é extremamente relevante já que cada vez mais os algoritmos operam de forma independente, ou seja, sem a participação direta de humanos. Observa-se a atuação deste tipo de inteligência artificial em processos seletivos para empregos, na aplicação de tarifas de planos de saúde, na obtenção de crédito, na indústria do varejo e do entretenimento, dentre outras. Conforme já destacado, os processos automatizados, como a construção de perfis, repetem padrões de discriminação da própria sociedade, portanto, se não regulados potencializam o

aprofundamento das desigualdades sociais, políticas, econômicas de gênero e raça.

Apresentados os direitos previstos no Regulamento Geral sobre a Proteção de Dados, prossegue-se para seu próximo artigo que trata das possíveis restrições aos direitos previstos. A limitação deve considerar os direitos e liberdades individuais e só deve ser utilizada em casos de extrema necessidade social como por exemplo, segurança nacional, defesa e segurança pública. Além disso, a prevenção, investigação, detecção, ou repressão de infrações penais, ou a execução de sanções penais são incluídas como possíveis restrições de direitos. Outra exceção prevista é quando os Estados suprimem direitos e obrigações com o objetivo de proteger os titulares de dados, em casos como, por exemplo, proteção da saúde pública, ou resposta a crises humanitárias. Ainda assim, toda limitação de direitos deve ser justificada. Por fim, caso ocorra a quebra do sigilo dos dados de forma temporária e em regime de exceção, os titulares dos dados permanecem com o direito de invocar o direito de remoção dos dados, retificação e limitação do tratamento.

Cada pessoa pode acionar a Autoridade Nacional de Proteção de Dados para apresentar uma reclamação caso observe que tenha ocorrido uma infração. Além disso, caso não no obtenham retorno sobre o andamento da reclamação no prazo de três meses, o sujeito pode acionar judicialmente a própria autoridade de dados. Os titulares de dados também podem acionar judicialmente qualquer controlador, operador, ou terceiro que julguem estar infringindo a regulação, ainda que a via administrativa seja facilitada pela existência da Autoridade Nacional de Proteção de Dados. Por fim, cada pessoa pode se fazer representar por uma organização, ou associação sem fins lucrativos em casos judiciais. Esta possibilidade de representação contribui para que ações coletivas sejam ajuizadas junto à Autoridade Nacional de Dados, ou até mesmo na justiça de cada um dos países membro da União Europeia.

Como pode-se observar os direitos dos titulares de dados de fato permitem que as pessoas exerçam a autodeterminação informacional, que envolve ter controle sobre os próprios dados, e não apenas consentir tacitamente. A seguir procede-se para o quarto capítulo da regulação, que aborda as obrigações e responsabilidades dos controladores, operadores de dados, subcontratantes e todos atores que tratam dados pessoais.

2.1.4 – Obrigações e responsabilidades

Para cumprir com as obrigações previstas no regulamento, o 24º artigo estabelece que os responsáveis pelo tratamento tomem medidas organizacionais e técnicas para proteger os direitos dos titulares de dados e adotarem os princípios da regulação. Os controladores precisam demonstrar que cumprem medidas para garantir a privacidade por padrão e que tratam apenas os dados necessários

para um propósito específico.

Ressalta-se que demonstrar conformidade (*compliance*) com a regulação é a primeira das obrigações de todos os atores que trabalham com o tratamento de dados pessoais. Neste sentido a principal transformação técnica e operacional é adotar o princípio da privacidade por padrão e implementar mecanismos de pseudoanonimização. Estas medidas têm como objetivo cumprir com a determinação de processar apenas os dados necessários para uma finalidade específica.

Os controladores são obrigados a manter os registros de todas atividades de processamento e disponibilizá-las caso a Autoridade Nacional de Dados requeira. Estes registros precisam incluir o nome e o contato do controlador, os objetivos do processamento dos dados, as categorias dos titulares de dados, dos dados pessoais e dos recipientes; o período em que os dados serão armazenados e quando serão apagados, além de uma descrição sobre as medidas de segurança organizacionais e técnicas adotadas.

Uma importante transformação promovida pelo Regulamento Geral sobre a Proteção de Dados é a designação de um encarregado da proteção de dados. As organizações são obrigadas a indicar um encarregado de proteção de dados quando o tratamento é efetuado por uma autoridade pública, quando as atividades consistem em operações de monitoramento em grande escala, quando envolvem o processamento de dados sensíveis, ou dados pessoais relacionados a condenações ou ofensas criminais.

Diante da possibilidade que um processamento de dados possa causar risco aos direitos e liberdades, os controladores são obrigados a realizar uma avaliação de impacto sobre a proteção de dados. Esta avaliação é conduzida pelo encarregado de proteção de dados e é especialmente necessária se o tratamento dos dados envolver decisões automatizadas, a coleta de dados sensíveis e o monitoramento de espaços públicos em larga escala. No documento deve conter a descrição das operações de processamento dos dados, assim com a finalidade do tratamento, os riscos de ferir os direitos e liberdades individuais. Além disso, deve englobar as medidas adotadas para minimizar estas ameaças e demonstrar conformidade com a lei. Se a avaliação indicar que o processamento de dados pode resultar em altos riscos para as liberdades e direitos individuais, e que o controlador em questão não adota as medidas necessárias para minimizar estes riscos, ele se torna obrigado a consultar a autoridade de proteção de dados previamente, ou seja, não pode tratar os dados antes de realizar uma solicitação formal.

Os controladores também precisam auxiliar os titulares de dados a exercerem seus direitos. Isto significa que devem fornecer informações a eles, independentemente se os dados foram obtidos de forma direta, ou indireta. Quando os dados são recebidos diretamente os controladores devem informar sua identidade e forma de contato, os propósitos e bases legais para o processamento dos dados. Além disso, precisam notificar sobre quem são os recipientes dos dados, se pretendem

transferir os dados para fora da União Europeia e indicar quem é o encarregado de proteção de dados. São obrigados ainda a orientar sobre o prazo que os dados serão armazenados, os motivos pelos quais precisa daquelas informações e se os dados serão submetidos a decisões automatizadas. Quando os dados são recebidos de forma indireta, como por exemplo, fontes de dados públicos, os controladores precisam destacar a origem dos dados.

Necessitam cooperar com a Autoridade Nacional de Proteção de Dados e notificá-la em caso de violações. A liberação proposital ou não intencional de informações privadas pode ocorrer de várias formas, que envolvem desde invasões em banco de dados, à erros humanos como perda de dados, ou a realização de cópias não autorizadas. Os controladores têm um prazo de 72 horas para notificar a Autoridade Nacional de Proteção de Dados caso ocorra algum tipo de violação. Devem informar sua natureza, a quantidade de dados vazados e de que forma impactam os indivíduos. Precisam indicar ainda as medidas e providências tomadas, ou previstas, para minimizar o fato, e as informações de contato do encarregado de proteção de dados. Nestes casos, é indispensável que os controladores notifiquem os titulares dos dados sobre a violação de seus direitos com as mesmas informações fornecidas à autoridade de dados.

Os controladores são obrigados a obedecer às especificações de transferência de dados para fora da União Europeia, ou seja, só podem transferir informações sobre os cidadãos do bloco para países que adotam medidas de segurança, privacidade e proteção de dados semelhantes. No caso de controladores que trabalham com dados pessoais de cidadãos do bloco, mas cujas sedes se localizam foram da região, torna-se necessário indicar um representante legal que esteja fisicamente alocado na União Europeia.

Por fim, os operadores e terceiros também são obrigados a tomar medidas técnicas e organizacionais para se adequarem às regras do Regulamento Geral sobre a Proteção de Dados. Eles devem operar com base em um contrato, ou ato legal, que detalhe as atividades de tratamento, ou seja, sua duração, natureza, tipo de dado pessoal envolvido no processamento, dentre outras informações consideradas relevantes. Este documento é a comprovação de que o operador, ou o terceirizado, trabalha a partir das instruções do controlador. Além disso, eles são obrigados a garantir a confiabilidade e a segurança dos dados, tornar qualquer informação disponível caso o controlador requeira e processar apenas as informações solicitadas.

Ocorre que as grandes empresas de tecnologia – conhecidos como controladores conjuntos - desempenham múltiplos papéis no contexto do regulamento. São controladores a partir do momento que coletam dados em troca de uma conta gratuita de e-mail, ou para a participação em uma rede social, ou aplicativo. Também atuam como operadores e, muitas vezes como terceiros, ou recipientes. O debate sobre o papel destes atores será retomado adiante, quando abordaremos as obrigações e responsabilidades de cada um deles. Por isso, o 28º artigo da regulação estabelece que, se o operador

durante sua atuação passar a determinar a finalidade e os propósitos do tratamento de dados, ele se torna automaticamente um controlador, estando sujeito às mesmas responsabilidades e sanções.

Os operadores possuem dois grupos de obrigações. O primeiro deles é composto por deveres similares aos dos controladores tais como; garantir a segurança, adotar a privacidade por padrão, registrar as informações de processamento, indicar um encarregado de dados e um representante, colaborar com as autoridades de dados, notificar em caso de violação dos dados, proteger e informar os titulares de seus direitos e liberdades. O segundo grupo de exigências, que deve estar em conformidade com a regulação, tem base contratual e registra a relação do operador, ou terceiro, com o controlador. Importante destacar que um operador não pode contratar outro operador, ou um terceiro, sem o conhecimento e anuência do controlador.

Estas são as principais obrigações e responsabilidades dos controladores, controladores conjuntos, operadores de dados e terceiros. Para garantir que sigam a nova regulação foram instituídas medidas de conformidade e execução, assim como possíveis sanções descritas na próxima seção.

2.1.5 – Sanções, mecanismos de execução e conformidade

Cumprir com os requisitos legais estabelecidos pela regulação não é uma tarefa fácil no contexto das práticas de processamento de dados. Inclusive, por tratar-se de uma transformação profunda na mentalidade, na atuação e nas formas com que as organizações processam dados pessoais. Se antes a lógica do capitalismo de vigilância estava centrada na coleta indiscriminada de dados pessoais, ou quanto mais melhor, a regulação agora limita a finalidade da coleta, estabelece a privacidade por padrão e busca minimizar a quantidade de dados coletados. Por isso, estabeleceu-se um prazo de dois anos para que as organizações públicas e privadas se adaptassem às novas regras, ou seja, a partir de maio de 2020 acaba o prazo de tolerância para a adoção completa do regulamento.

Para garantir a aplicação da regulação os legisladores europeus estabeleceram mecanismos de execução – que envolvem uma série de instrumentos e medidas - para garantir a proteção dos dados pessoais e a conformidade legal das organizações, empresas e governos.

A primeira grande medida é a designação de organismos independentes de proteção de dados, com poderes e autoridade para monitorar e fazer cumprir sua aplicação. Ou seja, cada Estado deve estabelecer em seu território uma Autoridade Nacional de Proteção de Dados, independente do governo, ou seja, a nomeação de seus integrantes deve ser feita de forma transparente e ela deve ter autonomia financeira.

A Autoridade Nacional de Proteção de Dados é o órgão que recebe denúncias e reclamações dos titulares de dados, sendo responsável por seu acompanhamento e monitoramento, podendo inclusive acionar judicialmente os controladores e operadores, caso não obtenha respostas. Elas

dispõem de um certo número de poderes de investigação e punição dos controladores e dos operadores. As autoridades podem solicitar o acesso aos dados dos controladores, podem emitir notificações, além de ordenar o bloqueio, o apagamento, ou a destruição de dados tratados. No limite podem proibir o processamento de dados por parte de controladores, operadores ou terceiros.

Por sua vez, o Comitê Europeu de Proteção de Dados é composto pelos chefes nacionais de Autoridades de Dados, por supervisores europeus de proteção de dados. Seu papel principal é garantir a consistência e aplicabilidade do Regulamento Geral sobre a Proteção de Dados, mas também desempenha funções de assessoria, cooperação e conciliação entre as Autoridades Nacionais, além de ser responsável por estabelecer recomendações, melhores práticas e diretrizes. Neste sentido, o Comitê tem o papel de manter a consistência entre as decisões das Autoridades Nacionais de forma a garantir que não sejam contraditórias. Sendo assim, desempenha a função de promover ações conjuntas, de cooperação mútua entre as múltiplas instâncias de proteção de dados.

O Comitê Europeu para proteção de dados possui um papel central na condução conjunta com organismos nacionais e europeus para estabelecer códigos de conduta e mecanismos de certificação aplicáveis às empresas. Estes mecanismos são voluntários e funcionam como um selo de recomendação de que a organização está em conformidade com o regulamento. As regras vinculativas aplicáveis às empresas (*binding corporate rules*) são adotadas para indicar que a atuação da companhia está de acordo com o Regulamento Geral sobre a Proteção de Dados. Estas medidas têm o objetivo de facilitar com que as empresas e organizações se adaptem às transformações impostas pela regulação. São uma forma de comprovação por parte dos controladores e operadores de que suas atividades são realizadas em conformidade com os princípios de proteção de dados e com os direitos dos titulares de dados, que é a primeira de suas obrigações. Em outras palavras, os controladores não são obrigados a adotar os códigos de conduta, as certificações e regras vinculativas, mas ignorar estes instrumentos pode ser prejudicial, inclusive financeiramente.

O titular de dados que considerar ter sofrido dano pode acionar a Autoridade Nacional de Proteção de Dados e solicitar indenização do controlador, ou operador que violou seus direitos. Uma reclamação pode seguir vias judiciais ou administrativas. Na segunda opção, as Autoridades Nacionais podem estabelecer multas de até 20 milhões de euros, ou até 4% do total do faturamento anual mundial da empresa, o que for maior. O valor das multas varia de acordo com a natureza, gravidade e duração da infração. Ao aplicá-la a Autoridade Nacional deve considerar também se o controlador ou operador agiu de forma intencional, ou foi apenas negligente. Por fim, a regulação determina que as multas sejam proporcionais à infracção e, ao mesmo tempo, também eficazes.

Desde que entrou em vigência o Regulamento Geral sobre a Proteção de Dados foi utilizado em diversos casos, dentre os quais o mais conhecido é o do *Cambridge Analytica*, que obteve dados de milhões de pessoas do Facebook, utilizando as informações em campanhas políticas como a do

presidente estadunidense Donald Trump, e a da saída do Reino Unido da União Europeia, conhecido como *Brexit*.

A Autoridade de proteção de dados da Inglaterra, o *Information Commissioner's Office* (ICO) multou o Facebook em 500 mil libras[47] (cerca de R$2,58 milhões), apenas pelo vazamento de dados dos britânicos. Já a Itália, no mesmo caso, multou a empresa em 10 milhões de euros (R$45 milhões)[48]. Mas foi na sede da companhia, nos Estados Unidos, o valor mais significativo; 5 bilhões de dólares – R$22 bilhões - em multa aplicada pela Comissão Federal de Comércio (*Federal trade Comission*)[49]. Até o Brasil, por meio da Secretaria Nacional do Consumidor, puniu o Facebook em R$6,6 milhões pelo mesmo caso[50].

Outras condenações surgem em vários países da União Europeia, como por exemplo na França[51], que multou o Uber por vazamento de dados. Isto que demonstra que o regulamento é utilizado pelas autoridades locais. Entidades de direitos dos consumidores de sete países da União Europeia se organizaram para questionar as ferramentas de rastreamento incorporadas por padrão nos celulares com sistema operacional Android[52], pertencente à Alphabet. No início de 2019 a Autoridade Nacional Francesa - Comissão Nacional de Informática e Liberdade (CNIL) – multou o Google em R$ 213 milhões[53] por dificultar o acesso de seus cidadãos aos termos de privacidade da plataforma.

Com o fim do prazo de adequação das empresas em maio de 2020 a tendência é que haja menor tolerância com violações da regulação. Os impactos não são apenas em empresas locais, pelo contrário, na mira dos legisladores estão grandes corporações da FAMGA. O Regulamento Geral sobre a Proteção de Dados da União Europeia despertou a atenção de outros países do mundo para o tema, tanto no sentido de adaptarem seus negócios ao modelo europeu, como também de proteger seus próprios cidadãos de forma semelhante.

---

[47] UK fines Facebook £500,000 for failing to protect user data. Disponível em < https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica >. Acessado em 7/2/19.
[48] Itália multa Facebook em € 10 milhões por vender dados de usuários. Disponível em < https://g1.globo.com/economia/tecnologia/noticia/2018/12/10/italia-multa-facebook-em-euro-10-milhoes-por-vender-dados-de-usuarios.ghtml>. Acesso em 2/1/20.
[49] Facebook pagará multa recorde de US$ 5 bilhões por violação de privacidade. Disponível em < https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/facebook-pagara-multa-de-us-5-bilhoes-por-violacao-de-privacidade.ghtml>. Acesso em 2/1/20.
[50] Ministério da Justiça multa Facebook em R$ 6,6 milhões em apuração sobre compartilhamento de dados. Disponível em https://g1.globo.com/economia/tecnologia/noticia/2019/12/30/ministerio-da-justica-multa-facebook-em-r-66-milhoes-em-apuracao-sobre-compartilhamento-de-dados.ghtml. Acesso em 2/1/20.
[51] French data protection watchdog fines Uber $460,000 for data breach. Disponível em https://techcrunch.com/2018/12/20/french-data-protection-watchdog-fines-uber-460000-for-data-breach/. Acessado em 7/2/19.
[52] European consumer groups want regulators to act against Google tracking. Disponível em https://www.reuters.com/article/us-eu-google-privacy/european-consumer-groups-want-regulators-to-act-against-google-tracking-idUSKCN1NW0BS. Acessado em 7/2/19.
[53] Google é multado em R$ 213 milhões pela França por dificultar acesso a termos de privacidade. Disponível em <https://gizmodo.uol.com.br/google-multado-213-milhoes-franca-dificultar-acesso-termos-privacidade/>. Acessado em 7/2/19.

As multas milionárias e as indenizações para os titulares de dados indicam que será necessário transformar o modelo de negócios do capitalismo de vigilância, ou ao menos minimizá-lo a partir da adoção de medidas técnicas e organizacionais para implementar a privacidade por padrão. A coleta indiscriminada de dados pessoais, sem finalidade específica, deverá aos poucos cessar, ou obter o consentimento explícito dos titulares de dados.

Zuboff (2019) considera positiva a aprovação do Regulamento Geral sobre a Proteção de Dados da União Europeia. Por outro lado, acredita que "as pessoas que lutam com a miríade de complexidades de sua própria proteção de dados não serão páreo para as impressionantes assimetrias de conhecimento e poder do capitalismo de vigilância" (Zuboff, 2019, p.451). Neste sentido, a autora acredita que "depende de como as sociedades europeias irão interpretar a nova legislação nas cortes. Mas não será a redação da regulação que irá moldar sua interpretação e sim os movimentos populares" (Zuboff, 2019, p.454). De fato, mobilizações conjuntas auxiliam a pressionar mudanças. Por outro lado, considera-se que a legislação da União Europeia é um importante passo para a transformação do modelo de negócios de coleta, tratamento e comercialização indiscriminada de dados pessoais.

Devido a todos estes fatores é possível concluir que a abordagem da União Europeia com relação à proteção de dados pessoais é focada nos direitos dos cidadãos, na conformidade do setor privado e dos governos locais com a lei, além de ter um caráter didático. Ao determinar Autoridades Nacionais com poderes punitivos, a regulação acaba por desonerar o poder judiciário de decidir sobre questões já determinadas e acordadas.

Resultado de ao menos trinta e cinco anos de reflexão e construção – da Convenção de Estrasburgo, em 1981, à edição do regulamento em 2016 – trata-se do marco regulatório mais relevante quando o tema é a privacidade e a proteção de dados pessoais. Justamente por isso sua análise será fundamental para as próximas etapas do trabalho, em que serão mapeadas as principais controvérsias em torno destes temas. Antes de prosseguir, é importante destacar como o tema é abordado pelas normas dos Estados Unidos e do Brasil.

2.2 – Marcos normativos dos Estados Unidos

Nesta seção destaca-se como o tema da privacidade e proteção de dados pessoais é compreendido na perspectiva estadunidense. Em primeiro lugar, é preciso destacar que nos Estados Unidos o debate sobre a proteção de dados pessoais tem uma abordagem bastante distinta da União Europeia, a começar pelos próprios termos utilizados. O tema é tratado como privacidade de dados (*data privacy*) retirando os sujeitos do protagonismo, ou seja, trata-se da privacidade das informações e não das pessoas. Em segundo lugar, é uma abordagem que não parte dos direitos humanos e sim

dos direitos do consumidor, ou do livre comércio e o conjunto de leis concorrenciais (antitruste). A terceira premissa importante são os ataques de 11 de setembro de 2001, que influenciaram diretamente na suspensão de legislações de proteção de dados e privacidade, em nome da guerra contra o terrorismo. Justamente por isso, boa parte do marco regulatório do país data da década de 1990. Por fim, há de se considerar que é um modelo que aposta na auto regulação do mercado, com o mínimo de interferência do Estado, o que faz com que o poder judiciário seja recorrentemente acionado.

Nos Estados Unidos não há uma lei geral de proteção de dados, mas uma série de regulações distintas, algumas inclusive cuja finalidade original não é a proteção de dados, mas questões envolvendo menores de idade, saúde e crédito, por exemplo. Outras leis remetem à questão da privacidade diretamente, mas, em sua maioria, buscam regular setores econômicos específicos como o sistema financeiro, a comunicação eletrônica e o sistema de saúde. O caminho legislativo não é preventivo, mas reativo, ou seja, as leis surgem após a solução de casos jurídicos específicos (Movius e Krup, 2009). O sistema privilegia o comércio e a segurança do Estado em prol dos direitos individuais, caracterizando-se como um modelo extremamente neoliberal, em que o estado intervém o menos possível, atuando de forma discreta na proteção dos direitos (Cobb, 2016). De fato, quando busca proteger os cidadãos o faz tratando-os como consumidores.

Não existe uma agência ou autoridade nacional responsável pela proteção da privacidade ou proteção de dados. Estes temas são tratados, ou pela justiça, ou pela Comissão Federal de Comércio (*Federal Trade Commission)*. A agência é responsável pela execução de políticas de privacidade e segurança no país, por produzir uma série de diretrizes sobre políticas de privacidade e por multar empresas que ferem a legislação.

Antes de prosseguir, é importante contextualizar o direito concorrencial e o direito dos consumidores. O primeiro tem suas bases ocidentais ainda na Grécia e Roma antigas. Por exemplo, o império romano era detentor do monopólio do sal nas regiões em que dominava (Bagnoli, 2002). Portanto, no modelo clássico concorrencial é preciso a concessão estatal para a exploração dos mercados. Durante o mercantilismo ocorre a distinção entre monopólios lícitos e ilícitos (Bagnoli, 2002). A crítica com relação ao papel do Estado na regulação dos mercados é inaugurada com a clássica metáfora de Adam Smith e a "mão invisível", em 1776. Para o autor, a lei da oferta e da procura é suficiente para a auto regulação dos mercados, sendo desnecessária a intervenção estatal. A própria economia de mercado está baseada no equilíbrio entre a oferta e a procura, que resulta em redução de preços e aumento da qualidade dos produtos. Ocorre que nesta equação não está prevista a formação de cartéis, o abuso de poder econômico e a conformação de monopólios privados, que prejudicam os consumidores.

As principais legislações que versam sobre a defesa da concorrência nos Estados Unidos são o *Sherman Act,* de 1890 e o *Clayton Act* de 1914. O primeiro tornou ilegal contratos que restringiam

o comércio com o intuito de formar monopólios. Já o segundo, regulou a fixação de preços, negociações casadas e a aquisição de empresas concorrentes. Estes marcos normativos partem do entendimento de que "a concorrência é fundamental para a competição de mercado e bem-estar econômico do consumidor" (Bagnoli, 2002, p. 234). Estas leis tinham como foco a regulação do mercado, não necessariamente os consumidores, mas foram responsáveis pela criação da Comissão Federal de Comércio.

Os direitos do consumidor levariam ainda alguns anos para se conformarem, representando um segundo aspecto da regulação do livre mercado. Trata-se de um conjunto de leis que buscam garantir o direito dos consumidores em ter um comércio justo, informações precisas e opções de mercado. Nos Estados Unidos, o marco histórico dos direitos do consumidor é o discurso do presidente John Kennedy, em 1962, no qual ele apresenta quatro direitos básicos; a segurança, o direito à informação, de livre escolha e o direito de ser ouvido (Almeida *et al*, 2002). Estes direitos se consolidam a partir de uma série de legislações como; a *Federal Food, Drug, and Cosmetic Act*, de 1938, que determina a segurança alimentar; a *Fair Debt Collection Practices Act*, de 1977, que busca reduzir o abuso na coleta de dívidas, dentre várias outras. Ao longo dos anos, os direitos dos consumidores englobariam ainda a satisfação mínima, direito à reparação, a educação do consumidor e o direito a um ambiente saudável.

Além destas legislações comerciais, existem leis que tratam diretamente sobre proteção de dados e privacidade. Uma das é o *Fair Credit Reporting Act* (FCRA), de 1970, editada para promover a exatidão, justiça e privacidade da informação do consumidor. De forma semelhante, há o *Financial Services Modernization Act,* de 1999. Esta e outras normas são voltadas para o cadastro positivo ou negativo – ou seja, se as pessoas podem, ou não, receber crédito de bancos e outras instituições financeiras. Estes marcos regulatórios tratam da privacidade de forma tangencial, buscando de fato regular o mercado, o sistema financeiro e o direito dos consumidores.

O tema é encaminhado de forma mais direta pelo *Federal Privacy Act*, de 1974, que regula as bases de dados do governo e que garante que a privacidade é um direito pessoal. De forma semelhante, destaca-se a *Electronic Communications Privacy Act*, de 1986, que estendeu às tecnologias digitais as mesmas restrições aplicadas a interceptação de comunicações telefônicas.

A fragmentação da legislação faz com que o sistema judiciário seja acionado com frequência (Cobb, 2016). No âmbito da Suprema Corte dos Estados Unidos foram julgadas várias ações sobre privacidade, já que é um direito que não é explicitamente garantido constitucionalmente. O entendimento da Corte recorre à quarta emenda, que garante "o direito do povo à inviolabilidade de sua pessoa, casas, papéis e haveres", defendendo em mais de uma ocasião que ela se aplica ao direito à privacidade.

A privacidade, ao ser abordada por várias legislações específicas, é garantida em uma série de

situações, mas a despeito do entendimento da suprema Corte, não é um direito universal, estando sujeito a falhas (Cobb, 2016). Em comparação com a abordagem europeia pode-se dizer que no velho continente a privacidade é um direito por padrão, enquanto nos Estados Unidos é um direito, em determinadas situações (Cobb, 2016). Na impossibilidade de listar ou legislar uma infinidade de possibilidades em que há a necessidade de proteger dados pessoais o direito à privacidade fica em suspenso, refém de uma autoridade que regula o comércio.

Na década de 1990, quando a Internet se comercializava, foram editadas uma série de leis com o objetivo de regulá-la. Dentre elas é editada a *Communications Decency Act*, de 1996, com o propósito de combater a pornografia *online*. Esta legislação abre precedentes para a questão da remoção de conteúdo *online*, especialmente a partir de sua seção 230, que determina que os provedores não podem ser responsabilizados pela publicação de terceiros. Ocorre que é uma lei anterior a indexação de conteúdo promovida pela web e o surgimento do fenômeno das redes sociais. A legislação é resultado justamente de uma controvérsia criada em torno de duas decisões judiciais contrárias à remoção de conteúdo difamatório na Internet (Zuboff, 2019, p. 109). Na prática, isto permite a criação de contas falsas em redes sociais, como Twitter, ou Facebook, a disseminação de conteúdo de ódio, o uso de robôs e outras práticas contemporâneas, que eram exceção em 1996, nos anos iniciais da Internet. Com isso, as grandes plataformas da *web*, que centralizam o fluxo de conteúdo, ficam isentas de responsabilização pela difusão de práticas que corroem o debate público.

Por outro lado, na década de 1990, talvez a mais importante legislação estadunidense sobre privacidade na Internet foi editada; a *Children's Online Privacy Protection Act* (COPPA), de 1998, que passou a vigorar a partir dos anos 2000. Criada para salvaguardar a privacidade de menores de 13 anos, a lei estabelece uma série de requerimentos que sites e aplicativos, dentre outros, devem estabelecer para a proteção dos dados desse público específico. Além de definir termos técnicos tais como informação pessoal, coleta e tratamento de dados, operadores e controladores, a lei introduz o conceito de "conhecimento real". Uma criança menor de 13 anos realmente sabe que está gastando o equivalente a um carro, ou uma casa em um jogo eletrônico[54]? Ou ela realmente precisa do consentimento dos responsáveis para navegar na Internet, baixar aplicativos e realizar outras atividades cotidianas nas mídias digitais? Pois a COPPA determina não apenas a necessidade do consentimento dos responsáveis devido à ausência de conhecimento real por parte de menores de idade, como determina a adoção de algumas práticas.

A primeira delas é a necessidade de criação de políticas de privacidade que descrevam quais informações são coletadas, com qual objetivo, se os dados são compartilhados com terceiros, e quais

[54] Garoto de 15 anos gasta mais de 100 mil reais em jogo online "gratuito". Disponível em https://www.tecmundo.com.br/video-game-e-jogos/63992-garoto-15-anos-gasta-100-mil-reais-jogo-online-gratuito.htm. Acessado em 7/2/19.

são os direitos dos responsáveis – já que menores de 13 anos não são titulares de dados. De forma semelhante à outras regulações, a lei estabelece multas em casos de violações, além de outras sanções, determinadas judicialmente ou pela Comissão Federal de Comércio. Em nível federal, a COPPA é o que há de mais avançado em termos de proteção de dados e privacidade nos Estados Unidos.

Inclusive, um grupo de trabalho da Comissão Federal de Comércio enviou um relatório ao Congresso[55], em 1998, sugerindo que alguns dos procedimentos e direitos previstos na COPPA fossem estendidos à todas as pessoas. Além disso, o texto sugeria estabelecer padrões para a coleta e tratamento de dados e a ampliação da capacidade da agência para atuar nas violações (Zuboff, 2019, p.112). O documento ainda "identifica princípios fundamentais de proteção de privacidade: (1) Notificação/Conhecimento; (2) Escolha/consentimento; (3) Acesso/Participação; (4) Integridade/Segurança e (5) Execução/Reparação". Observa-se a semelhança destes princípios com aqueles destacados pelo marco normativo europeu. Em suas conclusões, os comissários destacam que apesar da maioria das empresas estarem cientes da necessidade de proteger a privacidade de seus consumidores, muitos não haviam implementado as medidas de conformidade, ou seja, atuavam sem considerar as recomendações da agência.

O texto chegou a ser discutido no Congresso dos Estados Unidos, entretanto "meses de debate sobre privacidade simplesmente desapareceram da noite para o dia" (Zuboff, 2019, p.112), após os ataques de 11 de setembro. O incidente foi responsável por colocar a questão da segurança em primeiro plano nos mais diversos setores da sociedade, em especial do governo e do poder legislativo, que logo em seguida aos ataques editou o *Patrioct Act*. Esta legislação aumentou a capacidade de vigilância do Estado, seja por meio do aumento de buscas e apreensões, ou grampos judicialmente autorizados (Movius e Krup, 2009). Além disso, o *Patrioct Act* tinha como objetivo interceptar comunicações terroristas, o que levou às agências de segurança do país a focarem em um campo ainda pouco explorado; a Internet. Os resultados dessa legislação só revelaram sua real dimensão, quando Edward Snowden divulgou as práticas de vigilância em massa da Agência Nacional de Segurança estadunidense, em 2013. Estas são as principais legislações nacionais sobre privacidade e proteção de dados.

Portanto, desde os ataques de 11 de setembro de 2001 a prioridade do governo tornou-se a segurança, o que abriu espaço para que empresas realizassem um forte lobby – prática legalizada nos Estados Unidos - para que a privacidade e proteção de dados pessoais não fosse objeto de regulação nos anos seguintes (Zuboff, 2019). Com isso o sistema judiciário começou a ser acionado cada vez com mais frequência.

---

[55] Self-regulation and privacy online: A report to Congress. Disponível em https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf. Acessado em 7/2/19.

Em 1997, “o governo americano alegou que a Microsoft utilizava sua tecnologia para manter um monopólio ilegal” (Butts, 2009, p. 276). Isto porque o sistema operacional da empresa, o Windows, era acompanhado do navegador da empresa o Internet Explorer, o que prejudicaria outras companhias, à época sobretudo o Netscape que liderava o mercado. A iniciativa do governo foi muito criticada sob justamente o argumento de que o excesso de regulação nas novas tecnologias impediria inovações (Friedman, 1999). Em 2001, a Microsoft ganhou a ação abrindo precedentes para o entendimento de que empresas de tecnologia não abusam de seu poder econômico para direcionar as pessoas a consumirem seus próprios produtos. Alguns autores interpretam que “a escola de Chicago ensina que as leis antitruste existem para proteger os consumidores e não os competidores. Penalizar as práticas destas empresas como anticompetitivas reduziria a competição dinâmica” (Bork e Sidak, 2012, p.663). A decisão de fato criou uma jurisprudência com relação ao tema.

Por outro lado, esta não é a tendência das cortes europeias. Um caso semelhante expõe os diferentes pontos de vista. Em 2013, o Google foi alvo de investigação de órgãos de defesa dos consumidores dos Estados Unidos e da União Europeia “por favorecer seus próprios produtos nos resultados de busca em detrimento dos rivais” (Saldanha *et al*, 2018 p.77). Entretanto o entendimento das cortes foi divergente. No primeiro caso, a Comissão Federal de Comércio americana considerou que “não houve prejuízos à livre competição na manipulação dos resultados de buscas pelo Google (Saldanha *et al*, 2018 p.77). Já a Comissão Europeia condenou, em 2017, a empresa a “pagar uma multa de 2,42 bilhões de euros (cerca de R$ 8,97 bilhões). À época foi a maior condenação da história que envolveu gigantes da Internet” (Saldanha *et al*, 2018 p.77). Diante destes resultados pode-se concluir que;

> No modelo americano o direito à concorrência representa um princípio fundamental que justifica ações agressivas das empresas dominantes para ganhar mais vantagens competitivas. Já na experiência europeia, o direito anticoncorrencial surge em um contexto de aproximação dos mercados e de manutenção do bem-estar social. Nesse caso, a tutela jurisdicional recai menos sobre a competição e mais sobre os consumidores (Saldanha *et al*, 2018, p. 80).

Esta mesma lógica se aplica às abordagens americana e europeia com relação à proteção de dados pessoais e privacidade. Nos Estados Unidos a privacidade e a proteção de dados pessoais são temas de regulação comercial, ainda que a Suprema Corte invoque a quarta emenda da Constituição para defender os direitos individuais. É uma perspectiva ancorada no neoliberalismo, uma interpretação a partir da perspectiva da escola de Chicago (Butts, 2009). Ainda assim, é importante mencionar que ainda ocorrem investigações por violações das leis de antitruste do país[56], que podem obter desdobramentos diferentes da atual jurisprudência.

[56] Facebook e Google são investigados por práticas antitruste. Disponível em <https://www.dw.com/pt-br/facebook-e-google-s%C3%A3o-investigados-por-pr%C3%A1ticas-antitruste/a-50339717>. Acessado em 23/9/19.

Outra ação judicial relevante para o debate sobre privacidade e proteção de dados pessoais nos Estados Unidos foi a disputa entre a Apple e o FBI - *Federal Bureau of Investigation*)[57]. A empresa era pressionada pelas autoridades a fornecer dados sobre a comunicação privada de seus usuários. Diante disso, adotou a criptografia de ponta a ponta em mensagens privadas. Foi seguida pelo *Whatsapp*, que em 2014, incorporou o protocolo de segurança utilizado no *Signal*, aplicativo de troca de mensagens desenvolvido por Edward Snowden. Desta forma, as empresas se blindaram das ordens judiciais de quebra de sigilo ao alegar que não possuem acesso às mensagens, já que em teoria o conteúdo não fica armazenado na nuvem, sendo entregue diretamente aos destinatários finais. Portanto, a criptografia é fundamental para preservar a privacidade online[58]. No caso do FBI contra a Apple – que ainda envolveu o atirador de São Bernardino, em 2016 – o governo optou por retirar as solicitações[59]. Neste caso a disputa judicial acabou por beneficiar tanto os consumidores finais como as empresas.

Finalmente, contrariando o argumento do setor privado de que regular a proteção de dados e garantir a privacidade sobrecarrega a burocracia e abafa a inovação tecnológica está o caso da Califórnia (Cobb, 2016). Berço do Vale do Silício, é o estado americano detentor das legislações mais avançadas em termos de proteção de dados e privacidade. Foi o primeiro a editar uma lei sobre notificação em caso de violações de segurança, em 2003. Também foi pioneiro em reagir sobre a onipotente vigilância do Estado aprovando uma lei que limita a atuação do governo na interceptação de comunicações - *The California Electronic Communications Privacy Act* -, em 2016.

Além disso, em 2018, o estado aprovou o *California Consumer Privacy Act*, legislação que se aproxima do modelo europeu. Com vigência a partir de 1º de janeiro de 2020, este marco normativo tem como objetivo informar quais dados pessoais são coletados e se são comercializados e para quem. Com isto permite que as pessoas neguem a comercialização de seus dados pessoais e acessem quais informação são coletadas. Por fim, estabelece que os consumidores solicitem o apagamento de informações pessoais e que não sejam discriminados por exercerem seu direito à privacidade. Além de prever sanções como multas, por exemplo, a legislação inova ao determinar que na página inicial dos sites e aplicativos haja a opção de "não venda minhas informações pessoais[60]".

---

[57] Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.. Disponível em < https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html >. Acesso em 23/9/19.

[58] Without encryption, we will lose all privacy. This is our new battleground. Disponível em https://www.theguardian.com/commentisfree/2019/oct/15/encryption-lose-privacy-us-uk-australia-facebook?CMP=share_btn_tw. Acesso em 23/9/19.

[59] Justice Department Withdraws Request in Apple iPhone Encryption Case After FBI Accesses San Bernardino Shooter's Phone. Disponível em < https://abcnews.go.com/Technology/justice-department-withdraws-request-apple-iphone-encryption-case/story?id=37986428>. Acesso em 2/1/20.

[60] "Não venda meus dados": varejistas dos EUA correm para cumprir nova lei de privacidade. Disponível em< https://www.uol.com.br/tilt/noticias/reuters/2019/12/30/nao-venda-meus-dados-varejistas-dos-eua-correm-para-cumprir-nova-lei-de-privacidade.htm >. Acesso em 2/1/20.

Outros estados americanos também possuem leis locais sobre violação de privacidade e proteção de dados pessoais. Entretanto a *California Consumer Privacy Act* é considerada a legislação estadunidense que mais se aproxima do modelo europeu, devolvendo às pessoas o controle sobre as informações pessoais. Sua entrada em vigor retomou debate sobre uma lei nacional exclusivamente sobre privacidade, até o momento inexistente.

Por toda a complexidade dessa série de legislações, que ainda se confrontem com regras estaduais, pode-se concluir que o marco regulatório estadunidense não conseguiu alcançar um balanço entre a garantia dos direitos individuais e os interesses do comércio, abrindo brechas para práticas consideradas como ilegais na Europa. Este modelo confunde a segurança da informação com a proteção de dados pessoais, portanto privilegia a segurança em detrimento de direitos fundamentais. Por sua vez, a perspectiva europeia tem como foco os direitos humanos com características da social democracia, em que o Estado desempenha o papel de intermediário entre o setor privado e os direitos e liberdades individuais. Entretanto, conforme buscou-se demonstrar, trata-se de não apenas de marcos regulatórios bastante distintos, como de uma abordagem neoliberal que privilegia a segurança e o desenvolvimento tecnológico em detrimento da privacidade. Realizados estes destaques com relação aos marcos regulatórios estadunidenses e suas diferenças da abordagem europeia, prossegue-se para o contexto brasileiro.

2.3 – Privacidade e proteção de dados pessoais no Brasil

O debate sobre proteção de dados pessoais no Brasil ocorre, pelo menos, desde 2007, quando parte da sociedade civil se mobilizou contra um projeto de lei, que ficou conhecido como AI5 digital, em referência ao Ato Institucional 5, de dezembro de 1968, que marcou o endurecimento da ditadura militar[61]. O texto da proposta regulamentava a Internet no país pela perspectiva criminal e previa, dentre outras medidas, um cadastro de todos usuários de Internet no Brasil. O projeto ainda estabelecia facilidades de acesso a dados de navegação por autoridades policiais e determinava a criminalização de condutas corriqueiras na Internet, como por exemplo o compartilhamento de arquivos.

A mobilização contra o Projeto de Lei impulsionou o debate sobre direitos e deveres dos usuários da Internet no país, além de questões como a privacidade e proteção de dados. A discussão ocorria *online* em fóruns, blogs e listas de discussão, mas também em uma série de eventos

[61] Marco Civil da Internet: e você com isso?. Disponível em < https://revistagalileu.globo.com/Marco-Civil-da-Internet/noticia/2014/03/marco-civil-da-internet-e-voce-com-isso.html>. Acesso em 2/2/20.

presenciais. Dentre eles é importante recordar a 10ª edição do Fórum Internacional de Software Livre, ocorrida em Porto Alegre, em 2009, por uma série de fatores.

Na ocasião, foi lançado o portal Culturadigital.br, que viria a hospedar consultas públicas interativas como a do Marco Civil da Internet, do anteprojeto de lei de proteção de dados pessoais, dentre outras. O então presidente da república, Luís Inácio Lula da Silva foi ao evento, acompanhado da chefe da Casa Civil, Dilma Rousseff. Em seu discurso Lula se compromete em colocar em debate a questão dos direitos dos usuários da Internet no Brasil.

O resultado direto da presença de Lula no evento foi a criação de uma consulta pública na *web* para a construção do Marco Civil da Internet do Brasil[62]. No final de 2009, a consulta é lançada por meio da Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ), em parceria com a Coordenação de Cultura Digital, do Ministério da Cultura. Ela esteve aberta entre 29 de outubro de 2009 e 30 de maio de 2010 e obteve cerca de duas mil contribuições em forma de comentários, ou seja, era necessário ler e argumentar sobre as propostas, não apenas clicar em concordar ou discordar, por exemplo.

A consulta pública interativa do Marco Civil foi considerada um sucesso de participação por uma série de fatores, dentre eles o caráter de novidade, já que o governo federal nunca havia feito nada parecido na Internet (Santarém, 2010; Sampaio *et all*, 2013; Meireles, 2015; Solagna, 2015). Outras consultas públicas online tinham sido feitas pelo governo, mas em diferentes abordagens como formulários, recebimento de e-mails, dentre outros formatos fechados. Havia também a convergência entre forma e conteúdo, ou seja, era um debate sobre a Internet ocorrendo na *web*. À época os gestores do Ministério da Justiça optaram por elaborar um projeto de lei especificamente para tratar da privacidade online e a proteção de dados pessoais.

Em seguida à consulta do Marco Civil da Internet, a Secretaria Nacional do Consumidor (Senacom) em parceria com a SAL/MJ e o Observatório Brasileiro de Políticas Digitais do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas do Rio de Janeiro, lançam a consulta pública sobre a Proteção de Dados Pessoais no site culturadigital.br. O debate ocorreu entre 30 de novembro de 2010 e 30 de abril de 2011 e obteve 14 mil visitas e 795 comentários.

A consulta era muito parecida com a do Marco Civil da Internet em termos de formato – comentários intersticiais, ou seja, entre o texto do projeto de lei. O tema não era tão amplo como direitos e deveres dos usuários na Internet, mas relevante para ativistas que defendiam o direito à privacidade e proteção de dados na rede. Entretanto o resultado dessa primeira consulta foi um fiasco.

A começar pelo fato de que o texto final do anteprojeto de lei de dados pessoais sequer foi enviado ao Congresso Nacional, como ocorreu com o do Marco Civil da Internet. Além da

[62] Marco Civil da Internet. Disponível em < http://culturadigital.br/marcocivil/>. Acesso em 2/2/20.

participação reduzida, com a mudança de governo, em 2010, também foram trocados os gestores responsáveis pelo processo. Com isto, não ocorreu sequer um retorno aos participantes com relação às suas contribuições. De fato, em 2015, quando a SAL/MJ promove uma segunda consulta pública sobre o tema, o site original sequer estava no ar.

No intervalo entre as duas consultas, o Projeto de Lei foi modificado por diversos órgãos do poder executivo, entretanto sem uma sistematização das mudanças. Com isto, o Ministério da Justiça não publicou nada comparando as versões de 2011 com a de 2015, impossibilitando inferir sobre as contribuições dos participantes na primeira consulta.

Antes de prosseguir para a segunda consulta pública interativa sobre proteção de dados pessoais é importante contextualizar como ocorre a tramitação e aprovação do Marco Civil da Internet no Congresso Nacional. Após o término da consulta, a SAL/MJ consolida as contribuições e envia o projeto para a Câmara dos Deputados, em 24 de agosto de 2011. Ao chegar na Câmara dos Deputados o projeto do executivo se transforma no PL 2126/2011, com relatoria do deputado Alessandro Molon (PT-RJ).

Em 2012, o relator coloca o Projeto de Lei em debate no site e-democracia da Câmara dos Deputados em uma comunidade virtual que chega a 16.288 integrantes[63]. Após a consolidação das novas contribuições, o projeto passa por comissões especiais da Câmara e finalmente vai ao plenário, somando-se a milhares de outros projetos que tramitam na casa. A proposta só se transforma em prioridade do então governo Dilma Rousseff, após as revelação de Edward Snowden, em junho de 2013, de que a própria presidenta era alvo de espionagem por parte da Agência Americana de Segurança[64].

Entretanto, o Projeto de Lei do Marco Civil da Internet estava imerso em algumas polêmicas, dentre as quais duas são especialmente relevantes para o debate. A primeira, já mencionada quando apresentada o Regulamento Geral sobre a Proteção de Dados da União Europeia, refere-se à retirada de conteúdo da Internet. O texto final, que se tornou a Lei 12.965, de 23 de abril de 2014, em seu artigo 19º, privilegia a liberdade de expressão e deixa à cargo do poder judiciário a decisão sobre o mérito e licitude do conteúdo. Em outras palavras, com o objetivo de evitar uma censura prévia de conteúdo, a lei brasileira abre brechas para a omissão dos provedores de aplicações, já que estes só podem ser responsabilizados por danos decorrentes de conteúdo gerado por terceiros após ordem judicial específica. A lei do Marco Civil da Internet responsabiliza apenas a publicação original do conteúdo eximindo de obrigações as plataformas de conteúdo intermediárias.

---

[63] Marco Civil no e-democracia. Disponível em http://arquivo.edemocracia.camara.leg.br/web/marco-civil-da-Internet/inicio#.XFwapqpKjIV. Acessado em 7/2/19.
[64] Documentos da NSA apontam Dilma Rousseff como alvo de espionagem. Disponível em http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html. Acessado em 7/2/19.

O tema é realmente polêmico e o direito à liberdade de expressão deve prevalecer sob qualquer forma de censura. Conforme debatido na seção sobre privacidade e liberdade existem limitações ao direito da liberdade de expressão. É preciso refletir sobre o modelo brasileiro, especialmente diante da proposta alternativa do Regulamento Geral sobre a Proteção de Dados, em que a remoção de conteúdo ilícito é facilitada.

O segundo ponto polêmico foi o da neutralidade da rede, que significa que os provedores de aplicação devem tratar todos dos dados da mesma forma, sem privilegiar determinados tipos de conteúdo. Neste quesito havia um grande *lobby* das empresas de telecomunicação para a retirada da garantia da neutralidade da rede, de forma que pudessem comercializar planos que privilegiassem, ou tornassem mais caros, determinados conteúdos, em especial vídeos, que necessitam de mais conexão.

Inclusive em março de 2014, pouco antes do projeto ser aprovado, o então líder do PMDB na Câmara dos Deputados, Eduardo Cunha - que historicamente representou os interesses do setor de telecomunicações - apresentou um projeto de lei substitutivo ao Marco Civil. O novo texto retirava justamente a obrigatoriedade da neutralidade da rede[65]. À época havia muita pressão de diversos setores para a aprovação do projeto. O setor de telecomunicações demandava segurança jurídica para sua atuação no campo da Internet. A sociedade civil vinha de anos de mobilização para a garantia de direitos digitais. O governo se sentia vigiado pelas agências de segurança estadunidenses.

Após negociações no Congresso o projeto do Marco Civil da Internet foi aprovado[66] com a neutralidade de rede e a necessidade de ordem judicial para remoção de conteúdo na Internet. A lei do Marco Civil da Internet tem, dentre seus sete princípios, a proteção da privacidade e a proteção de dados pessoais. A legislação estabelece ainda como condição para o exercício do direito de acesso à Internet a liberdade de expressão e a privacidade. Portanto, ainda que não disponha especificamente sobre estes temas, inclusive devido a seu caráter abrangente – a lei é conhecida internacionalmente como a constituição da Internet, sendo modelo normativo para outros países, como a Itália[67] – eles estão previstos e mencionados.

Em 2015, a SAL/MJ lança paralelamente duas outras consultas públicas interativas; um novo texto de anteprojeto de Proteção de Dados Pessoais e a Regulamentação do Marco Civil da Internet. Ambas as consultas públicas recebem contribuições da sociedade civil, do setor de telecomunicações, da academia, de juristas dentre outros setores interessados no debate. O decreto que regulamenta o

---

[65] PMDB apresenta alternativa ao marco civil da Internet sem a neutralidade da rede. Disponível em http://www2.camara.leg.br/camaranoticias/noticias/COMUNICACAO/463614-PMDB-APRESENTA-ALTERNATIVA-AO-MARCO-CIVIL-DA-INTERNET-SEM-A-NEUTRALIDADE-DA-REDE.html. Acessado em 7/2/19.

[66] Câmara aprova projeto do marco civil da Internet. Disponível em http://www2.camara.leg.br/camaranoticias/noticias/COMUNICACAO/464530-CAMARA-APROVA-PROJETO-DO-MARCO-CIVIL-DA-INTERNET.html. Acessado em 7/2/19.

[67] Itália apresenta seu próprio Marco Civil. Disponível em https://exame.abril.com.br/tecnologia/italia-apresenta-seu-proprio-marco-civil/. Acessado em 7/2/19.

Marco Civil da Internet foi publicado[68] um dia antes do afastamento da presidente Dilma Rousseff, após a votação no Senado. No que se refere à privacidade e proteção de dados a regulação, além de definir o que são dados cadastrais, determina que eles só serão solicitados pelo governo por fundamentos legais, competência expressa e motivação para o pedido. O decreto também indica os órgãos responsáveis por fiscalizar o cumprimento da lei designando a Anatel e a Secretaria Nacional do Consumidor para a função. Importante enfatizar que na prática, a fragmentação das competências de fiscalização promove a ineficácia da lei, já que efetivamente nenhum dos órgãos exerce a função diretamente.

Por sua vez, o texto da segunda consulta do anteprojeto de lei de proteção de dados é consolidado pelo Ministério da Justiça, em parceria com o Comitê Gestor da Internet (CGI.br) e pesquisadores da Universidade Federal de Minas Gerais e publicado em 20 de outubro de 2015. Fortemente inspirado na legislação europeia o projeto obteve rápida tramitação no Congresso Nacional, impulsionado justamente pela entrada em vigor do regulamento europeu.

Em 29 de maio de 2018, apenas dias após a entrada em vigor do Regulamento Geral sobre a Proteção de Dados da União Europeia, a Câmara dos Deputados aprova o projeto que cria a Lei Geral de Proteção de Dados[69] . Novamente observou-se uma pressão de diferentes setores da sociedade para sua aprovação. A sociedade civil vinha mobilizada desde o Marco Civil da Internet, organizando inclusive a Coalizão Direitos na Rede, que reúne uma dezena de ONGs que defendem direitos digitais. O setor privado, que atua na área de Internet e telecomunicações, também tinha interesses em estabelecer uma segurança jurídica para suas atividades, em especial devido a vigência da regulação europeia. O Brasil, sem uma lei de proteção de dados, teria seu comércio eletrônico diretamente afetado pela regulação europeia. Ao adotar parâmetros de proteção de dados e privacidade semelhantes aos do bloco, o país somou-se a mais de cem outras nações que contam com uma lei geral de proteção de dados.

O projeto teve rápida tramitação no Senado. Após passar por comissões, foi aprovado sem modificações em 10 de junho de 2018, quando seguiu para sanção presidencial. Importante destacar que antes de sua aprovação, o Brasil possuía um marco jurídico semelhante ao estadunidense, com mais de quarenta leis que versavam sobre o direito à privacidade. Entretanto, a legislação sofreu alterações realizadas tanto por Michel Temer, em 2018, como por Jair Bolsonaro no ano seguinte. A seguir destacam-se os principais aspectos da legislação brasileira para, em seguida, ressaltar as alterações realizadas.

---

[68] Decreto nº 8.771, de 11 de maio de 2016. Disponível em < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acessado em 7/2/19.
[69] Câmara aprova projeto de lei de proteção de dados pessoais. Disponível em http://agenciabrasil.ebc.com.br/politica/noticia/2018-05/camara-aprova-projeto-de-lei-de-protecao-de-dados-pessoais. Acessado em 7/2/19.

2.3.1 – Principais aspectos e alterações da lei geral de proteção de dados

O texto aprovado pelo Congresso Nacional possui muitas semelhanças e algumas diferenças com o regulamento da União Europeia. Em seus dez capítulos a lei[70] destaca seus fundamentos, define como os dados pessoais podem, ou não ser tratados, estabelece as categorias de dados sensíveis, diferencia o tratamento de dados de menores de idade. Além disso, determina quando será o término do tratamento de dados, indica quais são os direitos dos titulares de dados. A norma diferencia as regras para o tratamento de dados pelo poder público e pela inciativa privada. Define quem são os agentes de tratamentos de dados pessoais – controladores e operadores – estabelecendo encarregados por seu tratamento, assim como as responsabilidades de cada um destes agentes. Define boas práticas de segurança e governança de dados, e quais sanções passives de execução em caso de violação da lei. Por fim, cria a Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados e da Privacidade, indicando suas atribuições e composição.

Seus fundamentos incluem o respeito à privacidade, a autodeterminação informativa (que vai além da necessidade de consentimento, englobando a noção de controle sobre os próprios dados), a garantia das liberdades, o exercício da cidadania e a inviolabilidade da intimidade. Ainda estabelece como fundamentos o desenvolvimento tecnológico, a livre iniciativa e a defesa do consumidor.

Em seu 4º artigo aponta as mesmas exceções para o tratamento de dados pessoais que a regulação europeia, como quando o tratamento é realizado por pessoa natural para fins particulares, para fins acadêmicos, de segurança pública, ou do Estado. Neste quesito a lei brasileira se diferencia do regulamento europeu em dois aspectos. Primeiramente, determina como exceções o tratamento de dados realizados para fins jornalísticos, ou artísticos e para atividades de investigação e repressão de infrações penais. Estas últimas serão objeto de uma lei específica.

O segundo aspecto é mais preocupante em termos de infrações aos direitos e liberdades fundamentais e a prática de discriminação. A regulação europeia aborda a questão do tratamento de dados pessoais para atividades policiais e investigativas englobando restrições e responsabilidades a elas. Já a lei brasileira, por sua vez, ao eximir a autoridade policial e jurídica das responsabilidades pelo tratamento de dados pessoais, abre brechas para o abuso destes agentes. Os agravos podem englobar a prática de criação de perfis, rotulando sujeitos com "tendências" de praticarem crimes, além de possibilitar com que os agentes de segurança nacionais atuem de forma "preventiva", vigiando determinas pessoas que considerem "perigosas". Neste sentido, a lei brasileira se aproxima do modelo americano, em que os direitos e liberdades são colocados em segundo plano em detrimento

[70] Lei nº 13.709, de 14 de agosto de 2018. Disponível em < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acessada em 7/2/19.

da “segurança nacional”. O tema é controverso e será aprofundado adiante.

Em seguida, o texto apresenta as definições dos principais conceitos envolvidos no tratamento de dados pessoais tais como; dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, titular, controlador, operador, encarregado, tratamento, consentimento, uso compartilhado de dados, autoridade nacional, dentre outros. A conceituação é idêntica ao regulamento europeu apresentada na seção 2.1.1 deste capítulo, portanto não é necessário repeti-las.

Assim como na regulação europeia, a lei brasileira determina dez princípios para o tratamento de dados, todos muito semelhantes, a saber; a finalidade, a adequação, a necessidade, o livre acesso dos titulares de dados, a qualidade, a transparência, a segurança e a responsabilização e prestação de contas, a não discriminação e a adoção de medidas preventivas. Dentre os princípios observa-se a ausência da privacidade por padrão, que afeta diretamente decisões técnicas e organizacionais dos setores que atuam no tratamento de dados pessoais. De fato, o termo “privacidade por padrão” não está diretamente mencionado em nenhum artigo da lei brasileira.

Em seu segundo capítulo, a legislação estabelece os requisitos para o tratamento de dados, em sua maioria bastante similares à regulação europeia, como a exigência do consentimento do titular de dados. Além disso, os dados pessoais podem ser tratados para as seguintes finalidades; para o cumprimento de obrigação legal, para a execução de políticas públicas, para a realização de estudos por órgão de pesquisa, para a execução de contratos a pedido do titular, para o exercício de direitos em processos judiciais ou administrativos, para a proteção da vida e tutela da saúde, ou quando necessário para atender aos interesses legítimos do controlador.

Importante questionar o que seria o legítimo interesse do controlador (em geral pessoas jurídicas, responsáveis pela coleta inicial dos dados). A lei aponta que o legítimo interesse do controlador deverá ter finalidade lícita e cita situações concretas como “apoio e promoção de atividades do controlador”. Neste sentido, práticas como spam, mídia direcionada, propaganda não solicitada, dentre outras, são atividades de promoção de controladores. De fato, Zuboff (2019) destaca como um dos desafios da implementação do Regulamento Geral sobre a Proteção de Dados da União Europeia justamente o argumento do legítimo interesse dos controladores, utilizado em batalhas judiciais. Para a autora este recurso “oferece uma oportunidade de passar por cima dos novos marcos regulatórios” (Zuboff, 2019, p. 456) já que pode ser interpretado como “o direito de empreender em determinada atividade econômica, ou até mesmo exercer a liberdade de expressão” (Zuboff, 2019, p. 456). A legislação europeia não abre essa exceção. Por isso, considera-se que o 10º artigo da lei brasileira, que dispõe sobre o legítimo interesse do controlador, beneficia o setor privado em detrimento dos direitos dos titulares de dados.

Feitas estas considerações é importante ressaltar que, dentre os requisitos para o tratamento de dados, a norma indica que poderão ser tratados para a proteção do crédito nos termos do Código

de Defesa do Consumidor. Como na regulação europeia, a lei estabelece regras mais rígidas para o tratamento de dados sensíveis e de saúde, assim como a necessidade de consentimento dos responsáveis no caso do tratamento de dados de menores de idade.

Em seguida, em seu terceiro capítulo descreve os direitos dos titulares de dados, muito semelhantes à regulação europeia. Dentre eles há a confirmação da existência de tratamento, o acesso aos dados, a retificação de informações, a portabilidade, a revogação do consentimento, a eliminação, ou anonimização de dados desnecessários e a possibilidade de fazer-se representar coletivamente.

Por outro lado, a lei brasileira não garante outros direitos previstos na norma europeia. Por exemplo, com relação às decisões automatizadas, ou seja, aquelas realizadas por algoritmos, a norma brasileira prevê que o titular de dados possa solicitar sua revisão, ou seja, permite que máquinas tomem decisões. No regulamento europeu as pessoas têm a autonomia de não se sujeitar a este tipo de tratamento de dados.

É relevante destacar este aspecto, pois as decisões automatizadas estão diretamente relacionadas à prática de construção de perfis. Como a lei brasileira estabelece a exceção do tratamento de dados por autoridades policiais e jurídicas, na prática, autoriza que estes agentes realizem este tipo de atividade. Há de se observar como isto impactará na crescente informatização da segurança pública e na ampliação do uso tecnologias como o reconhecimento facial.

Por fim, a lei geral de proteção de dados brasileira não prevê o direito do titular de dados de solicitar aos controladores, ou operadores a remoção de conteúdo, como prevê a legislação europeia. Neste contexto está mantido o que o Marco Civil da Internet determina, ou seja, o conteúdo só poderá ser removido mediante ordem judicial. Ocorre que desta forma, a legislação brasileira segue eximindo de responsabilidade as grandes plataformas de conteúdo, que operam como intermediários. As plataformas retiram conteúdo, ou contas de acordo com as próprias políticas e a seu tempo, sem a menor transparência sobre suas decisões, possibilitando fenômenos como a propagação de conteúdo falso, discurso de ódio, dentre outros.

Outra disparidade entre os modelos regulatórios é que a lei brasileira diferencia o tratamento de dados pelo poder público do tratamento realizado pelos controladores e operadores privados, instituições e do terceiro setor. O quarto capítulo da norma brasileira versa sobre o tratamento de dados pelo poder público, enquanto o sexto capítulo aborda o tratamento de dados por controladores e operadores não governamentais. Importante enfatizar que a regulação europeia não faz essa diferenciação, ou seja todos atores estão sujeitos à legislação. Na prática, a lei brasileira coloca o governo em uma categoria de exceções, o que abre precedentes para o uso indevido dos dados por parte do próprio Estado.

Muitos artigos que abordam o tratamento de dados pelo poder público foram vetados, ou alterados pela medida provisória editada ao final de 2018. Estas mudanças serão destacadas na

próxima seção. Por enquanto, indica-se alguns pontos positivos e outros preocupantes no que se refere ao tratamento de dados pessoais pelo poder público brasileiro.

De positivo, pode-se destacar que a lei prevê que as entidades do poder público, que tratam dados pessoais, deverão designar um encarregado de proteção de dados. Além disso, os dados devem estar em um formato interoperável, ou seja, a capacidade da informação de um determinado sistema se comunicar de forma transparente com outro sistema. Entretanto, neste mesmo artigo 25º, surge uma expressão que causa preocupação; "uso compartilhado". A norma diz que o compartilhamento deve respeitar os princípios de proteção de dados, além de atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas.

O compartilhamento de dados pessoais entre agentes do poder público é preocupante, ainda mais quando autoridades policiais e judiciais não estão sujeitas às regras da lei geral de proteção de dados brasileira. Efetivamente, abre a possibilidade para a distribuição de informações pessoais sensíveis entre os órgãos da administração pública. Um exemplo; a foto da carteira de motorista ser utilizada para reconhecimento facial em espaços públicos, por agentes de segurança.

Se o decreto que regulamentou o Marco Civil da Internet aponta que os dados pessoais de brasileiros só serão solicitados pelo governo por fundamentos legais, competência expressa e motivação para o pedido, a lei geral de proteção de dados vai em direção oposta. Somado à isso é importante destacar que, em junho de 2016, portanto antes do afastamento definitivo da presidente Dilma Rousseff, o vice editou o Decreto 8.789[71], sobre o compartilhamento de bases de dados na administração pública federal. Na prática, este decreto já permitia a distribuição de uma série de informações cadastrais entre os órgãos do poder executivo, colocando como exceção apenas dados sob sigilo fiscal.

Inclusive, em agosto de 2018, a comercialização de dados pessoais pelo serviço público brasileiro[72] tornou-se alvo de investigação por parte do Ministério Público, apurando inclusive a atuação do Serviço Federal de Processamento de Dados (Serpro). Portanto, a lei geral de proteção de dados brasileira, ao diferenciar o tratamento de dados realizados pelo poder público do setor privado, reforça o uso compartilhado de dados, fazendo com que o governo tenha potencialmente um amplo conhecimento acerca da vida pessoal e íntima de cada cidadão.

Como se o compartilhamento de dados pelo poder público não fosse suficientemente preocupante, em outubro de 2019, o governo editou um decreto[73] que institui o Cadastro Base do

---

[71] Decreto nº 8.789, de 29 de junho de 2016. Disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8789.htm. Acessado em 7/2/19.
[72] MPDFT investiga empresas que comercializam acesso a dados biométricos de brasileiros. Disponível em http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10261-mpdft-investiga-empresas-que-comercializam-acesso-a-dados-biometricos-de-brasileiros. Acessado em 7/2/19.
[73] Decreto nº 10.046, de 9 de outubro de 2019. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em 27/7/19.

Cidadão, reunindo mais de cinquenta bancos de dados de diferentes órgãos do poder público. A iniciativa se diz em conformidade com a lei geral de proteção de dados, entretanto inclui expressões alheias a ela, como por exemplo, “atributos biográficos” e “atributos biométricos”. A partir desta terminologia, observa-se que uso de dados sensíveis é ignorado, assim como o princípio da finalidade, que limita a coleta de dados. Na prática, o decreto determina que os dados pessoais dos brasileiros são propriedade do Estado, violando inclusive a Constituição de 1988, que protege a vida privada dos cidadãos. Realizadas estas importantes considerações sobre a ampliação do poder do Estado brasileiro de controlar os dados dos cidadãos, prossegue-se na análise da lei geral de proteção de dados.

As responsabilidades e obrigações dos controladores e operadores são semelhantes àquelas previstas na regulação europeia; devem manter registro das operações, estão sujeitas a elaboração de relatórios de impacto à proteção de dados pessoais, devem designar um encarregado de dados e atuarem em conformidade com a lei, determinar medidas de segurança, dentre outras.

A lei brasileira faz a mesma diferenciação que a regulação europeia entre controladores e operadores, sendo os segundos responsáveis pelo tratamento de dados conforme a orientação dos primeiros. Portanto, os controladores possuem mais responsabilidades que os operadores, já que são os que determinam a finalidade da coleta das informações. Ambos estão sujeitos ao ressarcimento de danos e a multas em caso de violação da lei, cujos valores ficam variam entre a 2% do faturamento da empresa, grupo ou conglomerado no Brasil, no seu último exercício, limitada ao total de cinquenta milhões de reais por infração.

Estes agentes devem adotar medidas de segurança da informação para evitarem violações, que, caso ocorram devem ser informadas em “prazo razoável” aos titulares de dados e à Autoridade Nacional de Proteção de Dados, com as principais informações sobre o incidente e medidas de reparação. A lei atesta que a Autoridade irá definir o que considera prazo razoável, entretanto pondera-se que poderia já ter adotado a regra de até 72 horas da regulação europeia.

Os últimos artigos da lei brasileira versam sobre a Autoridade Nacional de Proteção de Dados Pessoais. A autarquia era prevista desde o projeto de 2010, seguindo parâmetros de competência técnica, independência do governo e autonomia financeira, como é o modelo Europeu. A autoridade reuniria as atribuições de fiscalizar, aplicar multas, oferecer certificações, estabelecer diretrizes de melhores práticas, zelar pela aplicação da lei e regulamentar questões relativas à proteção de dados no Brasil. Além da autoridade nacional, a lei prevê a criação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, com representantes do poder executivo, do Ministério Público, do Senado e da Câmara, do Comitê Gestor da Internet (CGI.br), do Conselho Nacional de Justiça. Além destes, outros quatro representantes do setor acadêmico e quatro da sociedade civil.

A lei geral de proteção de dados pessoais, aprovada pelo Congresso Nacional, pode ser considerada como um avanço para a proteção de dados pessoais, apesar de eximir o Estado brasileiro

de algumas obrigações impostas ao setor privado. Como foi elaborada a partir do regulamento da União Europeia, refletia em muitos aspectos esta legislação, garantindo alguns direitos aos titulares de dados e normatizando a atuação do setor privado.

De fato, a principal diferença entre as normas é com relação ao tratamento de dados pelo poder público. Na União Europeia os governos dos Estados possuem as mesmas responsabilidades e obrigações que agentes privados de tratamento de dados, com exceções específicas como segurança nacional. Além disso, no âmbito da União Europeia as autoridades policiais e judiciais estavam incluídas entre os agentes de tratamento de dados, portanto sujeitos a regras e princípios da lei. Os titulares de dados, por sua vez, tinham garantido o direito de suspender o tratamento de dados por parte do governo se algumas das exceções previstas ocorressem.

Por sua vez, a lei brasileira cria uma categoria diferente para o poder público no que se refere ao tratamento de dados pessoais. Somado a isso, facilita o compartilhamento de dados pessoais entre órgãos administrativos. Não suficiente, exclui autoridades policiais e judiciais das regras presentes na lei. Desta forma, potencializa o poder de vigilância do Estado brasileiro e de seus agentes de segurança, em detrimento dos direitos dos titulares de dados. Com isto, aproxima-se assim do modelo estadunidense, que beneficia o setor privado e o próprio Estado. Sendo assim, pode-se considerar que a lei geral de proteção de dados pessoais brasileira é um marco regulatório importante, entretanto débil em regular a atuação do próprio Estado.

Ocorre que a norma sofreria alterações por vetos presidenciais e pela Medida Provisória 869[74], de 28 de dezembro de 2018. Estas alterações foram analisadas pelo Congresso Nacional no primeiro semestre de 2019, retornando ao executivo, que vetaria novamente alguns artigos. O texto final da lei foi sancionado em 9 de julho de 2019[75], com treze novos vetos presidenciais. Dentre eles, seis foram revogados pelo Congresso, que concluiu sua análise no início de outubro de 2019[76]. Sendo assim, apresenta-se a avaliação crítica do texto final da lei após sua tramitação.

A principal alteração da lei é com relação à Autoridade Nacional de Proteção de Dados, citada cinquenta e três (53) vezes no texto da norma, sendo considerada sua espinha dorsal, ou seja, essencial para que a legislação seja aplicada. A independência financeira do órgão, sua autonomia com relação ao governo e seu caráter técnico, lhe garantiam as características previstas no Regulamento Geral sobre a Proteção de Dados da União Europeia. É importante ressaltar que dentre os 120 países que contam com uma legislação de proteção de dados, apenas doze deles não possuem uma autoridade de

---

[74] Medida Provisória 869 de 28 de dezembro de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm#art1. Acessado em 7/2/19.
[75] Lei Geral de proteção de dados pessoais. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em 2/1/20.
[76] Congresso conclui análise de vetos sobre proteção de dados. Disponível em https://www12.senado.leg.br/noticias/materias/2019/10/02/congresso-conclui-analise-de-vetos-sobre-protecao-de-dados. Acesso em 23/9/19.

proteção de dados.

A Autoridade Nacional de Proteção de Dados deixa de ser uma autarquia, nos moldes de agências reguladoras, passando a estar vinculada à Presidência da República, de forma transitória. Após dois anos, o executivo pode torná-la uma autarquia, conforme previsto originalmente. Não serão destinados novos recursos para sua criação e os servidores serão indicados pelo executivo, ainda que o texto da lei assegure a autonomia técnica e decisória do órgão.

Portanto, inicialmente a Autoridade Nacional de Proteção de Dados não somente não terá independência do governo, como ficará diretamente ligada ao chefe do poder executivo. Somado a isso, não terá autonomia financeira necessária para fiscalizar a aplicação da lei, realizar as atividades de formação, treinamento e acompanhar as reclamações dos titulares de dados. Os efeitos de uma a Autoridade Nacional de Proteção de Dados vinculada e dependente da Presidência da República só poderão ser analisados a partir da entrada em vigor da lei, mas desde já se considera um dos principais retrocessos. A Autoridade vinculada à Presidência da República amplia o potencial de vigilância do Estado brasileiro amparado na lei, que diferencia o tratamento de dados pessoais do poder público de agentes privados.

Como consequência da alteração da natureza da autoridade, o novo texto modifica a destinação dos recursos arrecadados com as multas previstas na lei. Se, inicialmente, eram destinadas à própria autoridade, passam a integrar o Fundo de Defesa de Direitos Difusos, criado para reparação de danos ao consumidor, gerido pelo Ministério da Justiça. Outra modificação do artigo 52º, que versa sobre as sanções previstas na lei, é a possibilidade de conciliação direta entre os controladores e titulares de dados que tiverem seus dados vazados.

A terceira alteração é com relação ao tratamento de dados sensíveis, em especial por agentes de saúde (artigos 7º e 11º). O texto final ampliou o tratamento deste tipo de dado de "profissionais de saúde" para "serviços de saúde", além dos já previstos serviços sanitários. Além disso, foi revogado o parágrafo que previa que o titular de dados fosse informado "das hipóteses em que será admitido o tratamento de seus dados", o que fere o direito de ser informado sobre a utilização das informações pessoais. Foi incluído um parágrafo que prevê que o tratamento posterior de dados "poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos", ampliando assim a possibilidade de reutilização das informações. Por outro lado, a legislação deixou explicito que os planos de saúde não podem criar modalidades de planos, ou excluir usuários a partir do acesso aos dados.

Outra mudança é com relação ao encarregado de proteção de dados. O texto original determinava que a função fosse exercida por uma pessoa "natural". A redação final suprime essa palavra, com isto os controladores e o próprio poder público, podem indicar pessoas jurídicas para o exercício da atividade, o que retira a responsabilidade de que os agentes tenham em seu quadro interno

uma pessoa encarregada da função. Foi vetado ainda o artigo que "garantia da autonomia técnica e profissional no exercício do cargo". A justificativa do executivo foi que era considerada uma interferência do Estado na contratação de entes privados. Com isto, o encarregado de proteção de dados não necessita ter autonomia e conhecimento técnico para atuar.

Por outro lado, a supressão do termo "natural" é mais grave em outro trecho da lei: O artigo 20º, que versa sobre a possibilidade de o titular de dados solicitar revisão de decisões tomadas exclusivamente com base em tratamento automatizado de dados. A redação final retira o termo "pessoa natural". Portanto, mantém a garantia do direito de revisão, mas não necessariamente realizada por seres humanos. Ou seja, na prática, significa que se uma pessoa solicitar a revisão de uma decisão automatizada, esta poderá ser feita justamente de forma automatizada.

Ocorreram alterações ainda com relação ao problemático compartilhamento de dados, em especial por parte do poder público. O texto final do artigo 18º cria uma exceção para informar aos titulares de dados quando isto ocorre; "os casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional". A imprecisão da expressão "esforço desproporcional" é semelhante à de "legítimo interesse", ou "prazo razoável" já criticadas. Com isto, abrem espaço para interpretações subjetivas como, por exemplo, a proposta de alteração do código penal que eximia crimes cometidos por policiais sob "violenta emoção".

De forma semelhante, o 28º artigo, que previa que "a comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade", foi vetado. Ou seja, foi eliminado o direito do titular de dados de ser informado sobre o uso compartilhado – entre órgãos do poder público – de suas informações. No texto original, as pessoas seriam notificadas caso o Ministério da Saúde compartilhasse suas informações com o da Justiça, por exemplo. Este veto significa a total ausência de transparência do poder público sobre o compartilhamento de informações da população entre seus próprios órgãos.

Não suficiente, o novo texto abre outra possibilidade para o uso compartilhado de dados entre órgãos do poder público; "na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades" (inciso V do artigo 26º). Novamente observa-se uma abstração que abre precedentes para que dados sejam compartilhados. Além disso, o texto final manteve a autorização de compartilhamento de dados pessoais por agentes privados "quando houver previsão legal ou a transferência for respaldada em contratos". Em teoria, tudo que é feito no âmbito da administração pública é respaldado em contratos, portanto, observa-se novamente certa imprecisão na norma.

De forma similar, foi suprimido o artigo que protegia os dados das pessoas que solicitassem informações do poder público por meio da Lei de Acesso à Informação (LAI) e "vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado" (Inciso II do art. 23º). Este dispositivo havia sido criado para minimizar retaliações aos sujeitos que exercessem

pressão por meio da LAI para maior transparência da atuação governamental. Portanto, as pessoas que solicitarem informações por meio da LAI não apensas serão identificáveis, como poderão ter seus dados compartilhados com entes privados.

Sendo assim, o saldo do trâmite legislativo não foi positivo se considerado o texto inicial da lei, especialmente no que se refere à autoridade nacional de proteção de dados e o compartilhamento de dados pelo poder público[77]. Nos dois primeiros anos a autoridade estará vinculada à própria presidência da república, o que enfraquece a fiscalização do órgão com relação ao próprio Estado. Além disso, os titulares dos dados perderam direitos, dentre eles o de revisão humana de decisões automatizadas e de serem informados sobre o compartilhamento de dados entre o poder público e o privado, respaldado em contratos.

A norma brasileira confere muitos poderes ao Estado, que deve ter o interesse presumido da coletividade. Entretanto, ao posicionar a autoridade nacional de proteção de dados junto ao chefe do poder executivo acaba por conferir estes poderes ao governo. Somado a isso, se o compartilhamento de dados pessoais pelo poder público já era relativamente preocupante, a redação final da lei tornou esta prática alarmante. Neste sentido, a lei geral de proteção de dados pessoais é quase uma "lei geral de entrega de dados pessoais ao Estado brasileiro".

Diante destas alterações, pode-se argumentar que mesmo originalmente elaborada nos moldes do Regulamento Geral sobre a Proteção de Dados da União Europeia, a redação final lei brasileira tornou-se um marco regulatório mais próximo do estadunidense, no sentido de dar poder ao Estados sobre a gestão dos dados. Os princípios normativos elencados não condizem com a nova redação do texto, que oferece ao Estado brasileiro os dados de seus cidadãos. Há de se considerar ainda o decreto que cria o Cadastro Base do Cidadão, e o caráter autoritário do governo eleito em 2018. Estes elementos indicam que os dados pessoais dos brasileiros serão utilizados para finalidades pouco transparentes.

Realizadas as análises de três marcos normativos sobre proteção de dados pessoais e privacidade – da União Europeia, dos Estados Unidos e do Brasil – destaca-se a seguir um quadro comparativo entre eles.

---

[77] Coalizão Direitos na Rede repudia os 9 vetos de Bolsonaro à lei que cria a Autoridade Nacional de Proteção de Dados. Disponível em < https://medium.com/@cdr_br/coaliz%C3%A3o-direitos-na-rede-repudia-os-9-vetos-de-bolsonaro-%C3%A0-lei-que-cria-a-autoridade-nacional-de-ee536f6baeb>. Acesso em 3/3/20.

Quadro 2: Comparação principais aspectos dos marcos regulatórios.

Países e regras	**União Europeia**	**Estados Unidos**	**Brasil**
Órgão regulatório de fiscalização e aplicação de sanções.	Autoridades Nacionais independentes e autoridades Europeias de coordenação.	Comissão Federal de Comércio.	Secretaria Nacional do Consumidor (MJ), ANATEL e Autoridade Nacional vinculada à presidência.
Direito de não ser objeto de decisões automatizadas.	Há previsão. É necessário consentimento explicito para ser realizada.	Não há previsão legal nas normas federais.	Não há previsão, além disso, a revisão de decisões automatizadas pode ser feita automaticamente.
Direito de retirar os dados pessoais de cadastros (Opt-out).	Há previsão, com exceções.	Não há previsão legal nas normas federais.	Há previsão, com exceções.
Utilização de dados pessoas para novas finalidades.	A norma proíbe o uso de dados para novas finalidades.	Existem restrições a partir da Federal Privacy Act.	A lei prevê exceções que possibilitam a reutilização de dados pessoais.
Informação ao titular sobre o uso dos dados pessoais.	O regulamento estabelece que os titulares sejam informados do uso dos dados.	Existem restrições a partir da Federal Privacy Act.	A lei permite o uso compartilhado dos dados sem informar aos titulares.
Remoção de conteúdo.	Regime de notificação e retirada (*notice and take down*).	Ordem judicial com base na seção 230 do *Communications Decency Act*, de 1996.	Ordem judicial – Marco Civil da Internet.
Responsabilização de intermediários.	Responsabilidade compartilhada entre publicação original e plataformas de conteúdo.	Apenas publicação/autor original.	Apenas publicação/autor original.
Acesso aos dados pelo poder púbico e autoridades policiais.	Regras valem igualmente para autoridades de investigação e executivo com pequenas exceções voltadas ao interesse público.	Legislação nacional com base na Federal Privacy Act e no Patrioct Act, que amplia o acesso aos dados por agentes de segurança.	Potencializa o compartilhamento de dados entre órgãos do poder público e cria exceções para poder público e sistema de segurança.
Criação de perfis (*profiling*).	Só podem ser feitas mediante consentimento explícito do titular de dados.	Não há legislação nacional.	Prática não é proibida na legislação nacional.

Fonte: A autora a partir dos marcos regulatórios analisados.

O resumo do quadro comparativo indica que na União europeia os direitos dos titulares de dados têm mais garantias que nos modelos estadunidense e brasileiro. Além disso, nestes últimos o

poder de vigilância do Estado é muito pouco regulado. Por fim, uma característica exclusiva do marco regulatório brasileiro é a indicação de múltiplas instâncias de fiscalização – Anatel, Secretaria Nacional do Consumidor e Autoridade Nacional de Proteção de dados. Considera-se que a sobreposição de competências por parte de diversos órgãos afeta o cumprimento das leis e acaba por demandar do já sobrecarregado sistema judiciário brasileiro.

Realizadas estas ponderações, prossegue-se para a análise empírica que irá mapear o debate sobre privacidade e proteção de dados pessoais ao longo de treze anos nas sessões principais do Fórum de Governança da Internet. No próximo capítulo será apresentada a metodologia de análise, que de forma resumida, buscará mapear as principais controvérsias em torno do conceito de privacidade, a partir da combinação de métodos quantitativos e qualitativos. Com isto, busca-se cumprir o objetivo principal da tese que é mapear as principais controvérsias em torno do debate sobre privacidade e proteção de dados pessoais e sua relação com as democracias contemporâneas. Além disso, propõe-se avaliar como os diferentes marcos normativos refletem, ou não características consideradas democráticas para as sociedades contemporâneas.

3 – Análise empírica e discussão

Nos dois primeiros capítulos do trabalho foi realizada uma revisão de literatura dos principais conceitos que estruturam o trabalho. Foram discutidas teorias da democracia, a conformação do capitalismo de vigilância, a dicotomia público/privado, o conceito de privacidade e algumas de suas dimensões. Em seguida, produziu-se uma avaliação comparativa dos principais marcos normativos da União Europeia, Brasil e Estados Unidos, que tratam da privacidade e proteção de dados pessoais e a forma como estas legislações refletem princípios democráticos.

Com o objetivo avaliar como as controvérsias ocorrem de fato entre a sociedade civil, as empresas de tecnologia e os governos, propõe-se a análise da evolução dos debates sobre privacidade e proteção de dados pessoais no âmbito do Fórum de Governança da Internet, considerado o principal evento mundial sobre tecnologias da comunicação e informação. A partir do objetivo principal da tese que é mapear as principais controvérsias em torno do debate sobre privacidade e proteção de dados pessoais e sua relação com as democracias contemporâneas, será empregada a metodologia de análise de discursos (Latour, 2012; Denzin e Lincoln, 2011; Babbie, 2015). Para tanto, serão adotados métodos combinatórios de análises quantitativas e qualitativas, além do arcabouço teórico e técnico mobilizado nos capítulos anteriores.

Além do referencial teórico do primeiro capítulo e da análise comparativa do segundo utiliza-se referências da bibliografia das ciências sociais, em especial da ciência política, sobre metodologia científica, análise de redes e de discursos, coleta e tratamento de dados, modelos de variáveis e construção de parâmetros e critérios (Kellstedt e Whitten, 2018; King *et al*, 1994). Sendo assim, a partir de um modelo combinatório de referências e técnicas quantitativas e qualitativas, delineou-se os procedimentos adotados para alancar aos objetivos propostos da pesquisa.

O recorte utilizado são as sessões principais das últimas edições do Fórum de Governança da Internet, que totalizam cento e sessenta e dois (162) eventos, entre 2006 e 2019. Com esta análise empírica busca-se mapear a evolução do discurso sobre privacidade, direitos e democracia, construindo parâmetros para um mapeamento sobre as principais controvérsias em torno destes temas. O recorte da análise dos discursos sobre privacidade e as visões sobre democracia e direitos neste evento se justifica por uma série de questões apresentadas a seguir.

Em primeiro lugar buscou-se a pluralidade e diversidade de pontos de vista, com o intuito de extrapolar a centralidade do discurso do norte global, focada principalmente no eixo Europa e Estados Unidos, observando também a mobilização de atores de vários setores da sociedade de inúmeros países. Em segundo lugar, por ser organizado no âmbito das Nações Unidas, em seu departamento de questões econômicas e sociais, o Fórum reúne autoridades locais e internacionais capazes de impactar o mundo social, as instituições e as normas jurídicas. A transparência – todas as sessões são transcritas

de forma padronizada e estruturada – é outra característica que justifica a análise dos discursos no âmbito do Fórum de Governança da Internet. Todos os arquivos estão disponíveis na página do Fórum[78], e a partir de 2009 algumas atividades também registradas em vídeo, com transmissão ao vivo e armazenadas para consulta no canal do Fórum do Youtube[79]. Portanto, as informações oficiais presentes na página do Fórum são a fonte de dados empíricos aqui analisados. Os arquivos se encontram em diferentes formatos, mas todos passíveis de tratamento. São documentos de texto que destacam o orador e intervenções do público, o que possibilita uma análise quantitativa e qualitativa do conteúdo.

Os procedimentos adotados para a análise foram combinatórios em técnicas quantitativas e qualitativas, que serão descritas no presente capítulo que está dividido da seguinte forma. Além desta breve recapitulação do que foi apresentado até então, em um primeiro momento busca-se contextualizar o Fórum de Governança da Internet e seu histórico dentro do ambiente das Nações Unidas e dos debates cobre tecnologia e sociedade.

Em seguida, apresenta-se a ferramenta de análise quantitativa, que consistiu um programa escrito na linguagem de programação *Python,* para identificar palavras chave, associadas à discussão teórica dos primeiros capítulos. Na sequência, destaca-se os procedimentos metodológicos utilizados na análise qualitativa dos discursos das principais sessões, ou plenárias, do evento. Os resultados são apresentados de forma conjunta e descritos ao longo dos anos.

A partir destas ferramentas metodológicas busca-se cumprir o objetivo principal do trabalho de mapear controvérsias em torno do debate sobre privacidade e proteção de dados pessoais e sua associação com as democracias contemporâneas. Além disso, dialoga-se com o objetivo específico de avaliar como diferentes marcos regulatórios de proteção de dados pessoais refletem princípios e valores democráticos.

A seguir apresenta-se um breve histórico do Fórum de Governança da Internet, destacando sua importância no debate sobre Internet e sociedade em âmbito global. Em 2001, a Assembleia Geral das Nações Unidas aprovou a proposta da realização da Cúpula Mundial sobre a Sociedade da Informação para tratar de questões relacionadas à expansão das tecnologias da comunicação e informação pelo mundo.

O primeiro evento ocorreu em Genebra, em 2003, e a segunda edição, em 2005, Túnis, na Tunísia. Ambos foram organizados pela União Internacional de Telecomunicações (*International Telecomunications Union*), considerada a organização internacional mais antiga do mundo, fundada em 1865 para negociar a alocação do espectro eletromagnético e a infraestrutura de comunicações.

---

[78]Internet Governance Forum. Disponível em < http://www.intgovforum.org/multilingual/tags/about>. Acessado em 6/4/18.
[79]Canal do Fórum no Youtube. Disponível em < https://www.youtube.com/user/Fórum>. Acessado em 14/11/18.

Em 2003, o evento reuniu representantes de 175 países, em um público de mais de 11 mil pessoas. Na ocasião, a Cúpula promoveu uma Declaração de Princípios de Genebra, intitulada "Construir a Sociedade da Informação; um desafio global para o milênio[80]". O documento agrega uma visão conjunta do futuro da sociedade da informação em 67 tópicos que englobam inclusão, direitos humanos, educação, acesso à informação e ao conhecimento, capacitação, segurança, diversidade cultural e linguística, cooperação regional e internacional e ética. A Cúpula de Genebra também aprovou um plano de ação que estabeleceu metas, linhas de ação, objetivos e uma agenda que determinou mecanismos de avaliação.

A segunda fase da cúpula ocorre em 2005, em Túnis, na Tunísia, com um público praticamente duplicado, com destaque para a participação da sociedade civil, que superou o número de representantes governamentais e do setor empresarial com relação ao evento anterior. A cúpula foi marcada pela pressão da comunidade internacional por um debate sobre a governança da Internet, principalmente devido ao fato de que a entidade responsável pelo controle dos endereços da rede, a Corporação da Internet para Atribuição de Nomes e Números (em inglês ICANN - *Internet Corporation for Assigned Names and Numbers*) estar associada ao departamento de comércio dos Estados Unidos. O objetivo era "globalizar" o órgão permitindo a participação de diversos setores da sociedade em sua gestão.

O resultado deste segundo encontro foi a determinação de que a Secretaria Geral das Nações Unidades criasse o Fórum e Governança da Internet, reconhecendo que a "abordagem da governança da Internet deveria ser inclusiva e responsiva[81]". Kofi Annan, então secretário geral da ONU, anunciou a criação do Fórum em 18 de julho de 2006. Na ocasião, foi criado o *Multistakeholder Advisory Group* (MAG) com 46 membros, que se encontram três vezes ao ano na sede da entidade em Genebra, realizando o acompanhamento das metas e definindo os temas a serem tratados nos Fóruns. O grupo tem uma estrutura que conta com presidente, vice e secretaria geral, escolhidos e nomeados pelo secretário geral da ONU após um processo de seleção aberto à toda comunidade.

O primeiro Fórum, ocorrido em Atenas, em 2006, contou com onze atividades. A partir do segundo encontro ocorreram eventos paralelos organizados da seguinte forma; workshops, reuniões das coalizões dinâmicas, fóruns de melhores práticas, reuniões multilaterais, sessões temáticas do país sede, sessões instantâneas, fóruns abertos, diálogos inter-regionais, sessões de boas-vindas e de microfone aberto. A seguir resume-se em uma tabela o histórico dos locais de realização do Fórum e

[80]Documentos da Cúpula Mundial sobre a Sociedade da Informação. Disponível em < https://www.itu.int/net/wsis/index.html>. Acessado em 14/11/19.
[81] Sobre o Fórum de governança da Internet. Disponível em < https://www.intgovforum.org/multilingual/content/about-Fórum-faqs>. Acessado em 14/11/19.

o tema principal de cada um deles, conforme disponível no site do Fórum, fonte das avaliações realizadas no trabalho.

Quadro 3: Lista dos locais de realização do Fórum e tema principal.

ANO	CIDADE	PAÍS	CONTINENTE	TEMA
2006	Atenas	Grécia	Europa	Internet Governance for Development
2007	Rio de Janeiro	Brasil	América Latina	Internet Governance for Development
2008	Haiderabad	Índia	Ásia	Internet for All
2009	Sharm el-Sheikh	Egito	Ásia	Internet Governance – Creating Opportunities for All
2010	Vilnius	Lituânia	Europa	Forum 2010 – developing the future together
2011	Nairóbi	Quênia	África	Internet as a catalyst for change: access, development, freedoms and innovation
2012	Baku	Azerbaijão	Ásia	Internet Governance for Sustainable Human, Economic and Social Development
2013	Bali	Indonésia	Ásia	Building Bridges – Enhancing Multi-Stakeholder Cooperation For Growth And Sustainable Development
2014	Istanbul	Turquia	Europa e Ásia	Connecting Continents for Enhanced Multistakeholder Internet Governance
2015	João Pessoa	Brasil	América Latina	Evolution of Internet Governance: Empowering Sustainable Development
2016	Jalisco	México	América Latina	Enabling Inclusive and Sustainable Growth
2017	Genebra	Suíça	Europa	Shape Your Digital Future!
2018	Paris	França	Europa	'Internet of Trust
2019	Berlin	Alemanha	Europa	One World. One Net. One Vision.

Fonte: Autora a partir de dados extraídos do site.

Como pode-se verificar, o Fórum foi realizado de forma distribuída entre os continentes, sendo o Brasil sede do evento em duas oportunidades. As quatro primeiras cidades sede do evento foram definidas ainda durante a Cúpula da Sociedade da Informação, visando extrapolar reuniões ocorridas no continente europeu. Ainda assim, a maioria dos eventos ocorreu neste continente, totalizando seis edições, seguido pelo continente asiático com cinco edições. Nos anos seguintes a escolha é definida a partir de articulações da ONU e o presidente do Fórum. Observa-se uma correlação entre a presidência do Fórum e seus locais de realização.

A cada ano o número de atividades aumenta, por isso, o recorte da análise focou nas sessões principais, que são exclusivas, ou seja, sem atividades paralelas. Ao dar ênfase nas sessões principais é possível realizar uma análise quantitativa sem viés, dado que como o número de atividades ao longo dos anos aumenta a ocorrência dos termos cresceria proporcionalmente. De fato, na primeira edição do evento contabilizou-se apenas onze atividades, enquanto na última elas chegaram a trezentos e quarenta e oito (348). Somado à isso, nem todas as atividades paralelas têm seu conteúdo transcrito e disponibilizado no site, o que impede sua análise.

As sessões principais englobam uma cerimônia de abertura e outra de encerramento, além de debates sobre temas centrais, tais como; segurança e privacidade, futuro da Internet, questões técnicas, painel de diversidade, direitos humanos e liberdade de expressão, dentre outros. Temas emergentes são abordados ao longo dos anos, tais como neutralidade da rede, evolução do modelo de governança, questões regionais, dentre outros. O levantamento documental do número de sessões principais dos Fóruns, da primeira edição em Atenas à edição de 2019, em Berlin, na Alemanha, totalizou 162 arquivos, organizados na tabela 1;

Tabela 1: Número de sessões principais do Fórum analisadas por ano.

Ano	**Arquivos**
2006	11
2007	14
2008	14
2009	14
2010	10
2011	9
2012	8
2013	9
2014	12
2015	13
2016	11
2017	12
2018	13
2019	11
TOTAL	**162**

Fonte: Autora a partir de dados extraídos do site.

Estes 162 arquivos foram baixados e convertidos em documentos de texto para que o programa pudesse realizar sua leitura. Os resultados foram comparados com os disponíveis online com a ferramenta de localização do próprio navegador, que destaca o número de ocorrências na página. Após os primeiros testes foi realizado um ajuste para que o programa lesse os termos independente se a palavra estava em maiúscula ou minúscula. Feito este reparo, considera-se que o código realizou de forma precisa a leitura dos termos pesquisados.

Após os primeiros testes e com os arquivos padronizados e estruturados por ano, aplicou-se o programa escrito em *Python* para identificar o número de ocorrências em que os principais termos de pesquisa eram mobilizados durante as sessões principais. O código simples e intuitivo, que contou com a colaboração do pesquisador João S. O. Bueno, é reproduzido a seguir.

```
import sys
import os
import csv

def procura_palavra(palavra):
    saida = open(f'dados_{palavra}.csv', 'wt')
    escritor = csv.writer(saida)
    escritor.writerow(['Palavra', 'Contagem', 'Arquivo'])
    for pasta, pastas, arquivos in os.walk("."):
        if "env" in pasta or  ".git" in pasta:
            continue
        if not "20" in pasta:
            continue
        for arquivo in arquivos:
            caminho = pasta + "/" + arquivo
            conteudo = open(caminho).read()
            conteudo_minuscula = conteudo.lower()
            contagem = conteudo_minuscula.count(palavra)
            escritor.writerow([palavra, contagem, caminho])
            # print(f"{palavra},{contagem},{caminho}")
    print("Concluído")
def principal():
    palavras  = ["privacy", "rights", "surveillance", "freedom",
"security"]

    for palavra in palavras:
        procura_palavra(palavra)

principal()
```

A versatilidade do programa permite a edição das palavras chave a partir de sua alteração dentro dos colchetes ao final do *script*. O algoritmo foi escrito para buscar palavras chave e exportá-las em um arquivo no formato de valores separados por vírgulas (csv), que permite a importação das informações e resultados em planilhas. O resultado dos dados extraídos estão no Anexo 1 do trabalho.

A partir do recorte proposto para o trabalho, o mapeamento de controvérsias em torno dos debates de privacidade no âmbito do Fórum de Governança da Internet, e do debate teórico realizado nos primeiros capítulos foram selecionados os seguintes termos; *privacy, security, surveillance, rights, freedom*, em português; privacidade, segurança, vigilância, direitos e liberdade. Estas palavras

chave indicam a evolução dos discursos ao longo dos anos, ao diagnosticar o número de vezes em que cada um foi mobilizado[82].

A partir dos diagnósticos dos dados quantitativos que apresentam uma análise de frequência dos termos pesquisados, a pesquisa se voltou para análise dos discursos, com o objetivo de mapear os argumentos mobilizados no debate em torno do tema da privacidade, direitos e princípios democráticos. A análise qualitativa partiu da seleção da atividade principal em que a palavra "privacidade" tem maior incidência em cada um dos anos. A opção metodológica se justifica pela centralidade do tema, tratado nos primeiros capítulos, sendo estruturante para o debate sobre os algoritmos e a democracia, além da divisão das esferas pública e privada.

Primeiramente, foi realizada a leitura de todas estas atividades. Em seguida, destacou-se os discursos que debatiam os principais conceitos da pesquisa. Por fim, identificou-se a evolução das controvérsias ao longo dos anos. O mapeamento dos espaços onde ocorrem as discussões, realizado a partir da análise dos discursos, tem como objetivo enfatizar as principais controvérsias, assim como a visão sobre direitos individuais e coletivos, mobilizada em torno do tema da privacidade. Portanto, a análise qualitativa teve como foco as atividades principais cujo tema tratasse de privacidade, totalizando treze sessões ao longo dos anos, conforme apresentado no quadro 3.

Quadro 4:As sessões principais do Fórum analisadas a cada ano.

Ano	**Sessão**
2006	Sessão de Segurança
2007	Sessão de Segurança
2008	Ampliando a Segurança, Privacidade e Abertura
2009	Segurança, Abertura e Privacidade
2010	Segurança, Abertura e Privacidade
2011	Segurança, Abertura e Privacidade
2012	Segurança, Abertura e Privacidade
2013	Questões emergentes vigilância na Internet
2015	Direitos Humanos na Internet
2016	Direitos Humanos ampliando a conversa
2017	Intervenções Locais, Impactos Globais: Como a Cooperação Internacional Multissetorial pode tratar das rupturas da Internet, da Criptografia e do Fluxos de Dados
2018	Cibersegurança, confiança e privacidade.
2019	Tecnologias emergentes e suas interfaces com a inclusão, a segurança e os direitos humanos

Fonte: Autora a partir de dados extraídos do site.

[82] Outros termos – "democracia", "autonomia", "cidadania" e "dados pessoais" - também foram pesquisados, mas obtiveram baixa recorrência.

Para cada uma das sessões analisadas foram adotados os seguintes procedimentos metodológicos; leitura e sistematização do conteúdo a partir da recorrência dos termos pesquisados e identificação dos participantes e seus respectivos setores; Sociedade civil, Governo, Organização intergovernamental, Comunidade técnica e Setor privado. As intervenções foram ainda divididas como palestrantes ou panelistas, moderação, audiência presencial e remota.

Apresenta-se a seguir os resultados das análises quantitativa e qualitativa de forma conjunta, indicando tendências e variações, além de discutir os principais resultados dos debates anuais em termos de controvérsias envolvidas no debate sobre privacidade e proteção de dados pessoais e sua relação com direitos e visões de democracia.

Em primeiro lugar apresenta-se o resultado analítico das controvérsias mapeadas ao longo dos anos no quadro 5. Em seguida, detalha-se como as discussões ocorreram expondo os dados quantitativos que subsidiaram a avaliação qualitativa.

Quadro 5: Evolução das controvérsias.

ANO	Principais controvérsias
2006	Dualidade entre segurança e privacidade, principal argumento mobilizado para justificar a vigilância.
2007	Como regular diferentes aspectos do setor de tecnologia?
2008	A privacidade é um direito humano fundamental? Qual é a responsabilidade dos intermediários sobre o conteúdo publicado na web, sejam eles provedores de serviços ou plataformas de conteúdo? A neutralidade da rede deve ser garantida?
2009	Como tratar a questão do discurso de ódio online e quais as limitações da liberdade de expressão? O direito ao apagamento dos dados pessoais deve ser garantido? Como contestar a cessão "voluntária" de dados pessoais realizada por meio dos termos de uso das plataformas digitais e garantir o consentimento informado limitando a finalidade da coleta de dados pessoais?
2010	Como combater a concentração de poder das plataformas de conteúdo, o controle privado da opinião pública e o fato delas estarem se tornando gatekeepers da rede?
2011	Como operam os filtros de conteúdo automatizados e de que forma os algoritmos categorizam perfis online? Quem são os "terceiros" com os quais as plataformas de conteúdo compartilham os dados pessoais a partir da autorização cedida nos termos de uso?
2012	Como contestar a privatização da aplicação da lei (plataformas operando como juízes e executores das regras/ termos de uso a partir de critérios comerciais e não democráticos como pluralidade e diversidade)? A vigilância online está causando auto censura e limitação do direito à liberdade de expressão?
2013	Diante da vigilância em massa, como garantir a criptografia nas comunicações interpessoais? É possível contestar o colonialismo digital, que concentra no norte global as empresas de tecnologia e os governos que as regulam?
2014	É o fim da privacidade? Estamos resignados a aceitar a vigilância?
2015	Qual é a responsabilidade corporativa na venda de tecnologias de vigilância? A privacidade é fundamental para o desenvolvimento da personalidade? Como garantir a privacidade diante da expansão da internet das coisas?
2016	Como combater as notícias falsas e seus impactos em processos eleitorais pelo mundo? Como operam os algoritmos responsáveis pela tomada de decisões com impacto no mundo físico? As legislações do norte global funcionam em países com diferentes contextos (colonialismo legal)? Como contestar a concentração de poder das plataformas web e do sistema financeiro?
2017	Como garantir a anonimização de dados e aumentar a criptografia nas comunicações interpessoais?
2018	Como assegurar a proteção de dados pessoais nas legislações sobre cibersegurança?
2019	Como garantir a privacidade por padrão em tecnologias emergentes?

Fonte: Autora a partir da análise empírica das sessões principais do Fórum de Governança da Internet.

3.1 – Anos iniciais; 2006, 2007 e 2008.

Em 2006, o Fórum de Governança da Internet ocorreu em Atenas, na Grécia. Dentre as atividades principais aquela em que o termo "privacidade" obteve mais ocorrências – totalizado vinte e seis (26) entradas – foi a intitulada "Sessão de Segurança", que ocorreu no dia 31 de outubro. Na ocasião, o termo "segurança" foi mobilizado cento e noventa e uma (191) vezes, "vigilância" apenas duas, "direitos" cinco vezes e "liberdade" uma única vez.

Este primeiro debate pode ser considerado como introdutório e de caráter contextual. Gus Hosein, representante da academia, abordou a dicotomia entre privacidade e segurança. Já David Belanger, da empresa AT&T tratou de questões relativas à segurança dos mercados. Integrantes de organização intergovernamentais, como Malcolm Harbour do Parlamento Europeu e Henrik Kaspersen do Conselho da Europa, destacaram o papel do setor privado na expansão da infraestrutura da Internet e como os governos atuam na mediação entre os interesses públicos e privados. Christiaan Van Der Valk, de uma empresa de segurança da Suécia, foi enfático em criticar o excesso de legislações e medidas de segurança impostas pelos governos, alegando que são contra produtivas e que afetam de forma negativa a própria segurança.

A participação da audiência enfatizou "ameaças vindas não apenas de criminosos como também de governos", destacando de forma indireta a questão da vigilância por parte do Estado. Outro participante reforçou o debate técnico sobre segurança e infraestrutura, com ênfase na continuidade e interrupção de serviços (apagões).

Em resposta aos questionamentos da plateia, Kaspersen, do Conselho da Europa, ressaltou a importância do debate sobre a interferência do Estado na construção da infraestrutura de rede, em grande parte deixada para o setor privado. O debate sobre a interferência dos Estados foi retomado sob o ponto de vista da determinação de padrões técnicos, como protocolos de segurança. O argumento de que a tecnologia avança com rapidez e que por isso o mercado deve se autorregular também foi mobilizado.

Nota-se que as principais polêmicas ficaram centradas na dicotomia entre segurança e privacidade. O principal consenso, que é um discurso que se repetirá ano após ano, é que as soluções para os desafios envolvendo a privacidade e segurança devem ser colaborativas e multisetoriais, envolvendo governos, sociedade civil e empresas. Dentre as controvérsias surgidas é importante destacar a crítica do público com relação à vigilância realizada pelos Estados. Outro tema que aparecerá de forma recorrente é a questão da regulação do setor de tecnologia. Feitas estas breves considerações sobre o início dos debates sobre privacidade, prossegue-se para o ano seguinte.

Em 2007, dentre as sessões principais analisou-se a atividade "Sessão de Segurança", que ocorreu no dia 14 de novembro no Rio de Janeiro. Na ocasião a palavra "segurança" foi mencionada

cento e cinquenta e quatro (154) vezes, “privacidade” apenas dezessete (17). O termo “vigilância” foi mobilizado apenas três vezes, “liberdade” em duas ocasiões e a palavra “direitos” obteve dez ocorrências. A seguir destaca-se as principais intervenções da sessão que repercutem argumentos mobilizados em torno das questões de privacidade, exercício de direitos e o papel do Estado.

As falas iniciais foram bem genéricas e ancoradas em retóricas como “é preciso combater a pedofilia online”, ou “precisamos acabar com as fraudes online e o terrorismo”, ou focaram apenas em aspectos técnicos, como por exemplo a Convenção do Conselho da Europa sobre Cibercrime, que na ocasião contava com a adesão de 43 países.

Com relação à participação do público, destaca-se a intervenção de George Greve, que enfatiza a relação entre segurança, controle e transparência. Para ele a segurança por meio da obscuridade pode parecer lógica, mas é uma ideia fundamentalmente falsa. Cita que, para a matemática, um sistema que se baseia no sigilo para garantir sua segurança acaba sendo menos seguro. Por isso, argumenta que é necessário ter controle por meio da transparência.

Outras duas intervenções da audiência ressaltam a necessidade de privacidade, destacando os mercados paralelos de venda de dados, algumas vezes realizados pelos próprios governos. Tomohiko Yamakawa, representante da associação de comércio do Japão, critica o excesso de regulação, que em sua visão é um dos maiores problemas enfrentados pelo setor privado. Para fechar o debate o presidente da mesa, Antônio Tavares, do CGI.br, resume que as questões de segurança, estabilidade, integridade e confiança devem proteger as pessoas, combatendo os cibercrimes, adotando leis para isso, mas do ponto de vista dos direitos humanos. Finaliza ainda destacando que são temas inter-relacionados em um contexto democrático.

Neste ano observa-se que o debate sobre privacidade e proteção de dados ainda é secundário nos discursos, que em sua maioria destacam questões de segurança e cibercrimes. Importante destacar algumas controvérsias que surgem neste ano e se repetem em outras edições. Dentre elas a polêmica sobre a regulação do setor de tecnologia. O argumento colocado por representantes do setor privado é de que o excesso de legislações impediria o desenvolvimento e a inovação. Diferentes perspectivas sobre esta questão estão diretamente associadas às visões sobre democracia e direitos. Em geral, o setor privado defende o modelo neoliberal de mínima interferência do Estado. Já representantes da academia, do terceiro setor e de agências intergovernamentais, como a Unesco, por exemplo, defendem algum tipo de regulação. A questão é qual o melhor modelo, dado o rápido avanço da tecnologia.

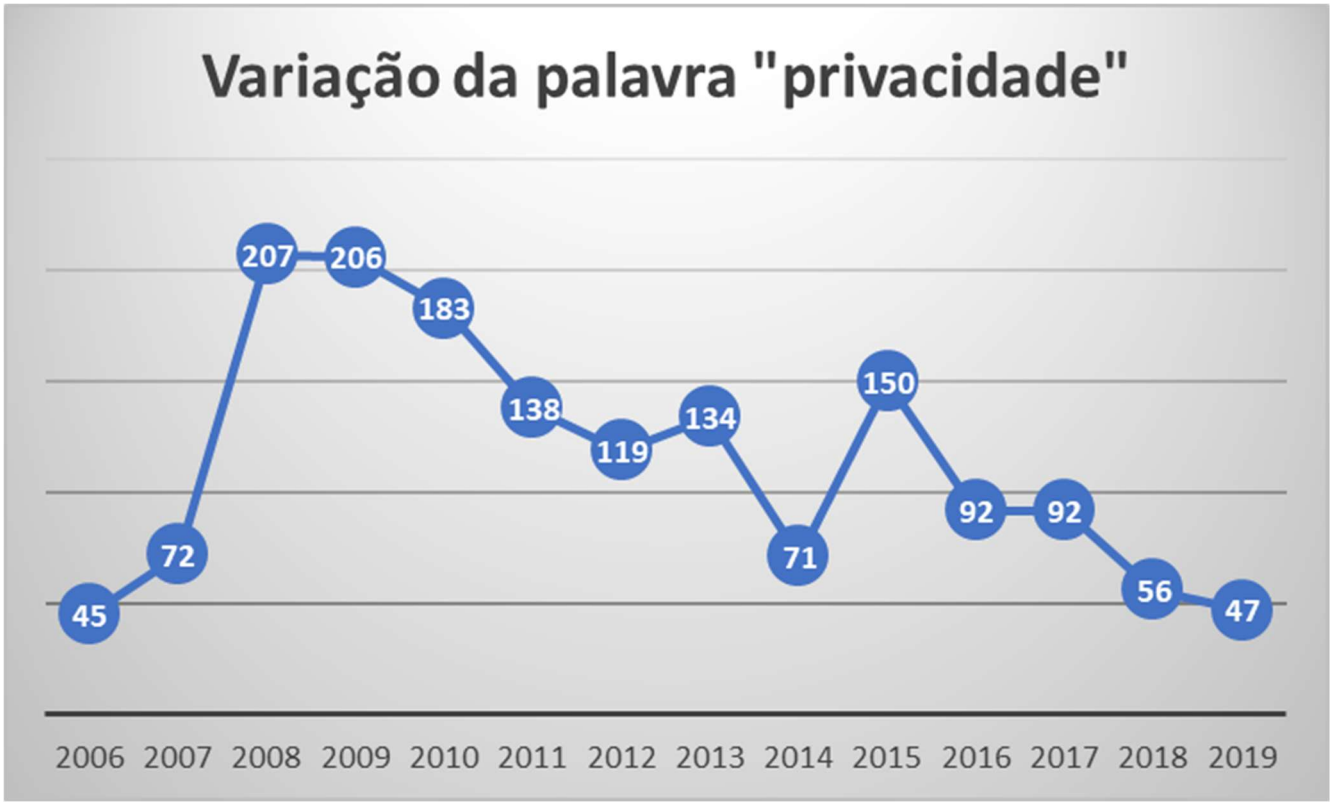
Dito isso, é importante destacar as intervenções do público que colocaram em pauta a questão da comercialização de dados pessoais e a relação da privacidade com o exercício da liberdade de expressão, tema que ganhará protagonismo nos debates dos anos seguintes. Outra importante questão que surge neste ano é a necessidade de transparência sobre a forma com que se realiza a segurança,

ou seja, os controles democráticos para que não haja abuso de poder. Realizadas estas considerações sobre os temas mais relevantes da sessão de 2007, prossegue-se para a análise do ano seguinte.

Em 2008, o Fórum de Governança da Internet ocorreu Haiderabad, na Índia. Dentre as atividades principais a que o termo privacidade foi mais mobilizado foi a intitulada "Ampliando a segurança, a privacidade e a abertura[83]" com quarenta e cinco (45) ocorrências. Esta sessão inaugura uma série de plenárias com o mesmo título até o ano de 2012, ou seja, por cinco anos. Na ocasião, a palavra "segurança" foi mobilizada trinta e nove (39) vezes, em menor número do que o termo "privacidade". Por sua vez, a palavra "direitos" obteve trinta e sete (37) ocorrências e "liberdade" dez (10) e "vigilância" apenas uma.

Este foi o ano em que o termo "privacidade" foi mais mobilizado nas sessões principais do Fórum de Governança da Internet, totalizando 207 ocorrências. Ao longo dos anos analisados a palavra "privacidade" é mobilizada mil seiscentos e doze vezes (1612) vezes e sua evolução é demonstrada no gráfico abaixo.

Gráfico 2: Mobilização do termo "privacidade" nas sessões principais do Fórum.



Fonte: Autora a partir de dados extraídos do site.

[83] Ampliando a segurança, a privacidade e a abertura. Disponível em <https://www.youtube.com/watch?v=6vxunsTTY50>. Acessado em 12/8/19.

O alto índice de 2008 se justifica pelo fato de que neste ano ocorreram duas sessões principais sobre segurança e, pela primeira vez, uma específica sobre privacidade. É notável ainda observar sua decaída ao longo dos anos, com exceção para 2013, quando ocorrem as revelações de Snowden e 2015, quando o tema sequer é título de uma sessão principal. Outro destaque é o baixo índice de 2019, que quase se iguala ao ano inicial de 2006. A variação do termo será aprofundada a seguir.

A avaliação qualitativa da atividade de 2008 apresenta algumas controvérsias. Dentre as falas iniciais dos palestrantes destaca-se a intervenção de Shyamai Ghosh, do conselho de segurança de seu país, que enfatizou que somado a segurança, privacidade e abertura há de se considerar também o direito à informação já que declaração universal dos direitos humanos contempla a importância do livre fluxo de informações.

Por sua vez, John Carr, representante da coalizão para segurança das crianças da Inglaterra, destacou cinco categorias de riscos que menores de idade estão expostos online; conteúdo inapropriado, questões relativas ao contrato (termos de uso), ao comércio online, o vício e a privacidade. Questionou como se pode obter o consentimento real de uma pessoa que não tem idade suficiente para dá-lo.

Jac Sm Kee, da ONG sul africana *Association for Progressive Communications* (APC) enfatizou que as mulheres que acessam conteúdo online precisam se sentir seguras e não se sujeitar a qualquer tipo de intrusão ou vigilância, seja das pessoas de sua própria comunidade (no contexto da violência doméstica), ou do Estado. Ela ressalta ainda que os direitos não são neutros ou não políticos.

O representante da empresa Oracle, Joseph Alhadeff, disse que todos querem que a segurança seja efetiva, que a privacidade seja respeitada e que é necessário um arranjo aberto para garantir a transparência e o livre fluxo de informações. Destaca que, quando se trata de privacidade e segurança, deve-se partir da possibilidade de se obter tecnologias e conceitos mutualmente fortalecidos, ou seja, uma configuração que otimize uma combinação de segurança e privacidade. De forma semelhante, deveria ser a abordagem sobre abertura e transparência, em sua opinião. Prossegue ponderando que, caso um sistema seja completamente aberto sobre sua configuração de segurança, pode colocá-la em risco, o que pode gerar tensões. O mesmo ocorre sobre ser completamente aberto sobre certos tipos de informação, que podem violar obrigações de confidencialidade com seus consumidores, empregadores e outros. Por isso, ele defende que as soluções fortaleçam mutualmente a privacidade e segurança.

Prosseguindo o debate, o representante da academia, Stefano Rodotà, destacou que a proteção de dados pessoais não se refere apenas à esfera privada das pessoas, mas sua própria liberdade. Ressaltou que dados coletados para determinados propósitos são utilizados para outros, e que neste contexto a proteção de dados pessoais deveria ser considerada um direito fundamental.

O representante da Unesco, Abdul Waheed Khan, deu ênfase ao artigo 19 da Declaração Universal dos direitos humanos, que se refere à liberdade de expressão e de imprensa. Afirmou que existem tentativas de reduzir estes direitos, seja por meios técnicos como, por exemplo, o filtro ou o bloqueio de alguns conteúdos, de forma financeira, como a imposição tarifas ou taxas, mas sobretudo iniciativas legislativas.

O moderador David Gross questionou os participantes sobre de quem é a responsabilidade em colocar limites e estabelecer regras. É papel do governo? São questões que o livre mercado pode determinar? Certas decisões devem ser delegadas às pessoas e famílias (como o acesso de crianças à Internet)? São algumas das questões levantadas. Alhadeff, da Oracle, respondeu que no mercado existem diferentes estilos de atuação e que as empresas fazem o que é mais apropriado para seu modelo de negócios, dentro das leis em que operam. Por sua vez, John Carr afirmou que as empresas têm responsabilidade se estão vendendo produtos que podem colocar menores em risco. Para ele, é dever do vendedor tornar os produtos seguros e que, no momento, as coisas não funcionam assim.

Rodotà ressaltou que os países da União Europeia têm uma preocupação com a proteção de dados e que é necessário adotar vários modelos em conjunto com todos os atores, ou seja de forma multissetorial. Alhadeff endossa a ideia de uma parceria público privada para abordar as questões de segurança e privacidade. Para ele a existência de regras corporativas obrigatórias são um mecanismo de *accountability*.

Sem abrir o microfone para a participação da audiência presente ou mesmo o remoto, após três horas de debate o moderador encerrou os trabalhos. Considera-se que a ausência de participação do público tornou o debate menos polêmico, por outro lado, nesta atividade são apresentadas duas novas perspectivas; a das mulheres e dos menores de idade, ambas por representantes do terceiro setor. Outro ponto importante que ganhará destaque ao longo dos anos é a limitação do uso de dados para finalidades não expressas durante sua coleta, ou seja, a reutilização de dados para outros propósitos.

Observa-se ainda o início da controvérsia sobre a privacidade ser um direito fundamental, ou não. Neste contexto é importante enfatizar que o tema da liberdade de expressão também surge, ainda que de forma tímida. Ele será central em anos posteriores e será retomado adiante.

Neste ano a controvérsia da regulação do setor de tecnologia se materializa no debate sobre a responsabilidade dos intermediários, sejam eles provedores de serviços (ISP – *Internet Service Providers*), ou plataformas de conteúdo como redes sociais e mecanismos de busca. Esta polêmica será central ao longo de todos anos nos debates sobre privacidade e proteção de dados do Fórum de Governança da Internet. A questão central é se estes intermediários podem ser responsabilizados sobre o conteúdo publicado pelos usuários.

Neste contexto vale ressaltar que dentre os princípios de governança da Internet do CGI.br está a inimputabilidade da rede, compreendida pelo órgão como "o combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos[84]". Este princípio tem como base o artigo 230 do *Communications Decency Act*, de 1996, que criou a jurisprudência que protege o setor privado da responsabilidade pelo conteúdo publicado pelos usuários.

Ocorre que, por outro lado, ao isentar estes atores de determinadas responsabilidades e obrigações ocorre uma ruptura no próprio ecossistema multissetorial da governança da Internet. O debate está intrinsecamente relacionado a questão da privacidade e proteção de dados pessoais, pois as empresas obtêm as informações dos consumidores e devem protegê-los. Desta forma, também se blindam das interferências de governos, ou regimes autoritários. Compreende-se que, supostamente, ao não ceder informações de seus consumidores para agências de segurança, ou para o sistema judiciário, as empresas estão protegendo a privacidade das pessoas. Ocorre que, como se verá ao longo dos anos, estas informações pessoais são utilizadas em benefício próprio, na criação do mercado de dados pessoais.

Em certa medida o tema da inimputabilidade de rede está relacionado a outro debate sobre neutralidade da rede, que se refere à não descriminalização de pacotes de dados, em outras palavras, que todos os dados transmitidos na Internet sejam tratados de forma igualitária. A neutralidade de rede garante a privacidade a partir do momento em que não identifica o tipo de conteúdo que cada pessoa consome online, impedindo que operadoras forneçam planos diferenciados. Ela é um dos princípios da lei do Marco Civil da Internet, que seria aprovado como lei no Brasil alguns anos depois. Por outro lado, a neutralidade da rede não é garantida na legislação estadunidense. Ambas controvérsias – responsabilidade dos intermediários e neutralidade de rede - se aprofundam ao longo dos anos conforme se observa adiante.

3.2 – Os anos das redes sociais; 2009 a 2012.

A atividade "Segurança, Abertura e Privacidade" de 2009, ocorreu no dia 16 de novembro, na cidade de Sharm el-Sheikh, no Egito. Nesta sessão o termo "privacidade" se sobressaiu sendo mobilizado cento e cinquenta e duas (152) vezes, seguido de noventa (90) ocorrências para o termo "segurança" e oitenta e três (83) vezes a palavra "direitos". "Liberdade" foi identificada vinte e seis (26) vezes e a palavra "vigilância" em duas oportunidades.

[84] Princípios de governança da Internet. Disponível em <https://principios.cgi.br/inimputabilidade-da-rede>. Acessado em 12/8/19.

Dentre as falas iniciais a da representante do governo da Sérvia, Jasna Matic, é relevante por destacar que o fenômeno das redes sociais estava remodelando o debate sobre privacidade. Ressaltou que todos atores – governo, empresas e sociedade civil – tem suas responsabilidades e que há uma preocupação específica com a segurança de menores de idade.

O representante do setor privado, Joseph Alhadeff, que participou da atividade do ano anterior, menciona que a Organização para a Cooperação e Desenvolvimento Econômico (OECD) possui diretrizes de segurança para garantir a conformidade das empresas, assim como sua transparência e *accountability*. Para ele, as empresas devem adotar estas diretrizes para ter credibilidade. Com relação aos novos modelos de desenvolvimento de produtos e sistemas, sejam eles conceituados como "*privacy by design*" ou "*secutiry by design*" ele defende um processo colaborativo, que envolva os consumidores, além de diversas disciplinas de administração e o contexto cultural e regulatório em que as empresas atuam.

Cristine Hoepers, do CGI.br, enfatiza que é necessário saber de quem se quer proteger o público em geral. Para ela um dos maiores problemas da atualidade é que as pessoas publicam informações online sem saber dos riscos envolvidos. Diz ainda que o design dos softwares é problemático e que as universidades não estão preparando os novos profissionais para elaborarem projetos seguros. Finaliza ressaltando que não é necessário comprometer a privacidade para ter mais segurança.

A representante da academia, Namita Malhotra, contribui para o debate a partir de uma perspectiva feminista. Para ela a privacidade está relacionada à autonomia pessoal. Recorda que a distinção público privada é um problema central do feminismo já que, dentre outros fatores, a noção de privado faz parte da opressão sistêmica que as mulheres sofrem ao redor do mundo. Neste sentido, pontua ainda que o privado é a zona não regulada da vida, sendo excluída dos principais debates públicos e políticos. Na mesma linha, enfatiza que os sistemas sociais e legais garantem a privacidade daqueles que poderiam muito bem levar as mesmas vidas publicamente, tornando o direito à privacidade uma questão de privilégio e hierarquia. Neste sentido, ressalta que corpos que não seguem padrões definidos como normais e 'saudáveis' não têm as mesmas garantias de privacidade. Enfatiza ainda a importância do conceito de consentimento no debate sobre privacidade e da peculiar noção da privacidade em público, temas retomados adiante na discussão.

O representante do setor acadêmico, Bruce Schneier, inicia sua fala indicando que estamos produzindo cada vez mais dados e que eles são propriedade de companhias de telefone e de cartão de crédito não estando sobre o controle dos próprios sujeitos. Ressalta ainda que, como a privacidade não é uma questão saliente, o mercado não consegue lidar muito bem com o tema e que, portanto, deve estar sujeita à legislação. Finaliza destacando que a privacidade é um direito humano fundamental.

Para o integrante do Conselho da Europa, Alexander Seger, a questão chave é como manter a segurança juntamente com o devido processo legal, a liberdade de expressão e a privacidade em um ambiente global em que cada país tem diferentes regras. O consultor da ONU sobre liberdade de expressão, Frank La Rue, reitera a complementariedade dos direitos e ressalta que todos os atores têm suas responsabilidades, mas enfatiza que o Estado é o responsável final por garantir o exercício dos direitos humanos. Para ele, o acesso à informação sobre temas de interesse público deve ser transparente. Destaca que a equidade e a justiça são princípios dos direitos humanos, assim como a pluralidade e a diversidade. Afirma que o acesso aos meios de comunicação não deveria ser um privilégio de poucos que podem adquiri-los, mas que deveriam estar acessíveis a todos, permitindo o acesso a diferentes pontos de vista. Por fim, enfatiza o princípio da limitação, ou da regulação estatal com vistas a garantir a possibilidade igualitária do exercício dos direitos humanos. Finalizando suas colocações iniciais, destaca que os artigos 19 e 20 da Declaração Universal dos direitos humanos, que tratam da liberdade de expressão, não deveriam permitir o discurso de ódio, ou incitação a qualquer tipo de discriminação e violência, com o cuidado de não cair na armadilha da censura.

Antes de abrir para a participação da audiência, o moderador Marc Rotenberg faz uma pergunta aos debatedores; qual é o principal desafio que o futuro da Internet enfrentará? Para Cristine Hoepers, representante da comunidade técnica, o desafio já está presente. Trata-se de separar entre o que é uma medida defensiva de segurança do que está se tentando apresentar como uma medida válida apenas para restringir algo ou coletar dados. Para Namita Malhotra trata-se do papel que grandes e poderosas corporações começaram a ter em termos de agregação de dados, que podem utilizá-los, ou vendê-los. Para ela, a privacidade precisa ser enxergada em camadas e o conceito de integridade contextual da informação pode ser uma abordagem interessante. Já Bruce Schneier diz que o desafio está em balancear os interesses dos poderosos – sejam eles governos ou grandes corporações - com o interesse dos outros.

Em seguida, o microfone é aberto para a participação da audiência presencial e remota. A primeira intervenção é de Steve DelBianco da organização *NetChoice*, que questiona se os direitos fundamentais são negociáveis, por exemplo, seus filhos adolescentes renunciam a sua privacidade por serviços gratuitos online. As repostas destacam que a privacidade é direito e não uma mercadoria, neste sentido se deve refletir sobre o que é um direito e o que é o controle sobre certos tipos de informação. Namita Malhotra retoma o conceito de integridade contextual da informação, explicando que uma informação oferecida para determinada finalidade não deve ser utilizada para nenhum outro propósito sem o devido consentimento.

A seguinte intervenção do público questiona qual o limite entre segurança e censura. O consultor da ONU, Frank La Rue, responde que é um limite difícil de se estabelecer, mas que deve ser feito à luz dos critérios de direitos humanos. Portanto, para ele, a lei deve ser estabelecida antes

de sua aplicação, que deve ser feita pelo poder judiciário, não o executivo, e muito menos como acontece atualmente na Internet, em que as regras são aplicadas por entidades privadas, contratadas pelo Estado para monitorar.

Outra intervenção da audiência é feita por Bertrand de la Chapelle, da *Information Society* francesa, que enfatiza que as mídias sociais estão redefinindo alguns elementos do que se considerava privacidade e a intimidade é um exemplo, já que atualmente as pessoas expõe suas informações pessoais de forma voluntária. Além disso, ele comenta que, para além dos tratados internacionais e leis nacionais, existem as regras desenvolvidas pelas empresas privadas na forma dos "termos de uso", que devem ser consideradas. Namita Malhotra responde diferenciando três tipos de dados; aqueles que as pessoas entregam às corporações, aqueles que compartilham uns com os outros, e aqueles que os sujeitos ainda podem controlar. Para ela, o ponto central é que as pessoas fornecem informações pessoais em diferentes contextos e que o uso destes dados deve estar limitado àquela finalidade. Joseph Alhadeff, representante do setor privado, segue um raciocínio semelhante destacando que são necessários modelos que considerem o consentimento para o uso dos dados para além do escopo inicial.

Na mesma linha da intervenção anterior, Thomas Schneider, da *Information Society* da Suíça, destaca o crescimento dos serviços gratuitos online, em que as pessoas não pagam uma taxa diretamente, mas indiretamente por meio da participação na categorização dos usuários. Neste sentido, ele questiona até que ponto deveria ser permitido que as pessoas escolhessem utilizar ou não estes serviços. Para ele, esta prática gera o risco de se criar uma sociedade de dois tipos; uma em que os ricos têm recursos e conhecimento para se proteger e outra dos pobres, que não possuem os recursos para tanto.

Da audiência Zahid Jamil, do Paquistão, questiona se algumas vezes as empresas são cúmplices das agências de segurança dos governos, sendo forçadas a tomar determinadas ações. Malhotra responde que é injusto enxergar as empresas como vítimas, porque elas são poderosas, e podem inclusive moldar legislações locais para atender a seus próprios interesses.

Outra intervenção do público feita por Stephen Lau, de Hong Kong, é com relação ao direito ao esquecimento e ao apagamento dos próprios dados quando solicitado. Schneier é categórico ao afirmar que tecnicamente não é possível apagar todos os dados, pois sempre haverá redundância. Por outro lado, é possível fazer isso por meio da legislação, pondera. Para ele, se existirem leis determinando o apagamento dos dados as empresas devem obedecer.

Mais adiante o integrante da plateia Pavan Duggal, da *Cyberlaw Asia*, argumenta que algumas mudanças estão ocorrendo como a explosão do uso de celulares, o aumento dos cibercrimes, o fenômeno da computação na nuvem e as redes sociais. Diante desse contexto ele questiona aos palestrantes se eles enxergam que os governos locais irão mudar seu ponto de vista sobre a

privacidade. Schneier responde que estas mudanças estão interconectadas, são interdependentes e extrapolam as fronteiras dos Estados. Por fim, os palestrantes fazem suas considerações finais e a atividade é encerrada.

Observa-se que em 2009, a sessão sobre privacidade e segurança e abertura agregou novas questões, extrapolando os discursos retóricos sobre a complementariedade da privacidade e segurança e a solução multissetorial dos problemas. Com isto, surgem novas controvérsias no debate que se relacionam diretamente com a privacidade, o exercício dos direitos humanos e com os princípios democráticos.

Com o fenômeno das redes sociais e tecnologias móveis se consolidando, os debatedores problematizam questões inerentes à cultura do compartilhamento, como o fornecimento voluntário de dados pessoais, os riscos envolvidos na auto exposição, a necessidade de consentimento para a reutilização de dados para outras finalidades e o próprio surgimento do mercado de dados. O tema do direito ao esquecimento é abordado, sendo à época uma polêmica devido ao caso do jornal espanhol *La Vanguardia* e Mario Costeja González, já citado. Além do direito ao esquecimento os participantes também enfatizam o direito ao apagamento dos próprios dados quando solicitado.

Neste ano a controvérsia sobre os termos de uso, o contrato realizado entre as pessoas e as empresas, é questionado a partir da perspectiva da integridade contextual da informação. Ou seja, as pessoas fornecem seus dados para determinada finalidade, mas as empresas, por meio de garantias estipuladas nos termos de uso, utilizam estas informações para outros propósitos, muitas vezes sem o consentimento informado, ou até mesmo o conhecimento das pessoas. Em outras palavras, estão livres para criarem suas próprias regras com pouca ou nenhuma intervenção por parte do Estado, além de se tornarem proprietárias dos dados das pessoas, que possuem pouco, ou nenhum controle sobre eles. Neste contexto, são relevantes as intervenções que enfatizam que as leis devem ser estabelecidas antes de sua aplicação, já que as regras dos termos de uso são determinadas pelas plataformas e modificadas de acordo com seus interesses. Portanto, o que acontece na Internet, onde as regras são estabelecidas e aplicadas pelo setor privado, é uma corrupção do próprio sistema democrático.

Importante destacar a intervenção da palestrante que se declara abertamente feminista, responsável por colocar em pauta a questão do consentimento informado e o fato de que o direito à privacidade é um privilégio de classe e raça. O tema é tratado pelo consultor da ONU de forma semelhante quando ele fala sobre o acesso aos meios de comunicação, que deveriam ser acessíveis a todos, mas estão concentrados nas mãos de poucos, o que viola princípios como o da pluralidade e diversidade. A assimetria de poder gerada pela concentração de recursos é uma das grandes controvérsias que envolvem o debate sobre democracia e o exercício dos diretos humanos, a privacidade e o mercado de dados pessoais.

Neste contexto surge outra grande controvérsia que se aprofundaria nos anos seguintes; a proliferação do discurso de ódio, a questão da retirada de conteúdo online, a liberdade de expressão e a censura. O tema está diretamente relacionado ao debate sobre a responsabilidade dos intermediários, apresentado na discussão do ano anterior, que questiona justamente o papel do setor privado diante dos novos desafios impostos pela expansão da tecnologia. O consultor da ONU enfatiza que o Estado é o responsável final por garantir o exercício dos direitos humanos, ou seja, deve aplicar o princípio democrático da limitação, regulando os setores para garantir que todas as pessoas exerçam seus direitos de forma igualitária. Com isto ele mobiliza uma visão sobre democracia em que o Estado exerce a regulação do setor privado, em contraposição à posicionamentos liberais que defendem a auto regulação do mercado.

Por fim, se consolida também o debate sobre a privacidade enquanto um direto humano, portanto inalienável, ou seja, não se pode renunciar a ele em troca de serviços, ou praticidades. Os discursos mobilizados entorno deste tema também refletem visões distintas sobre democracia e o exercício dos direitos. Posicionamentos mais liberais enxergam a privacidade a partir da perspectiva do direito dos consumidores, enquanto legislações europeias defendem a intervenção do Estado para garanti-la.

Identificadas novas controvérsias, prossegue-se para a análise qualitativa do debate de 2010, que ocorre em Vilnius, capital da Lituânia. A partir deste ano o formato das sessões principais deixa de ser o de painel e adquire características de plenária, já que se ampliam número de atividades paralelas, deixando a cargo das sessões principais a tarefa de agregar os principais debates.

Na plenária de 2010, o termo “segurança” foi o mais mobilizado com noventa e sete (97) ocorrências, seguido de “privacidade” com noventa e três (93), “direitos” com sessenta e cinco (65) e “liberdade” com cinquenta e quatro (54). A palavra “vigilância” não obteve nenhuma ocorrência. Em termos de discursos mobilizados, essa é a plenária em que mais pessoas foram ao microfone, ultrapassando trinta indivíduos, em menos de três horas. A atividade foi dividida em três grandes temas; o fenômeno das redes sociais, a natureza e características da infraestrutura de rede e a cooperação internacional.

Dentre as colocações iniciais, destaca-se a fala do consultor da ONU, Frank La Rue. Para contextualizar o debate, ele identifica como mídias sociais aquelas utilizadas de maneira não comercial e de forma voluntária na troca de pontos de vista e posições, como rádios e jornais comunitários, que prestam um serviço público à uma comunidade, portanto se diferenciam das plataformas de redes sociais da web.

Em contraposição, Cynthia Wong, do *Centre For Democracy and Technology*, representando o terceiro setor, afirma que as redes sociais são controladas pelos usuários, que possuem muitas escolhas com relação ao conteúdo que vão ver e interagir. Ela defende que as plataformas não sejam

responsabilizadas pelo mau comportamento de alguns usuários, já que diante dessa possibilidade as plataformas passariam a atuar como *gatekeepers*, vigiando seus usuários por temer represálias legais por parte dos Estados.

Por sua vez, o representante da academia, Giacomo Mazzone**,** compara as plataformas de conteúdo às regras dos meios de comunicação de massa. Ressalta que, nos contratos de concessão do sistema de rádio fusão existem obrigações, como, por exemplo, o provimento de serviço universal e a confiabilidade e segurança, o que faz com que a informação seja verificada, correta e justa. Além disso, em alguns países, há ainda o compromisso com a pluralidade e diversidade, com regras e obrigações para garantir o acesso e publicidade de minorias. Já na Internet, estas regras não se aplicam, dado que a audiência é medida de forma diversa, ou seja, por cliques, ou tempo de permanência em sites. Finaliza defendendo que é importante a adoção de índices e paradigmas de medição de conteúdo na web que valorizem a pluralidade e diversidade cultural e o interesse dos consumidores.

De forma semelhante, o representante do governo suíço, Thomas Snyder, destaca que as plataformas web cada vez mais despenham funções antes feitas de forma exclusiva por organizações de mídia tradicionais. Por isso, defende uma abordagem que leve em conta não apenas a organização, mas também a função que desempenha. Com relação à regulação, destaca que regras podem ser graduais, *ex post facto*, ou seja, constituídas após os acontecimentos, bem como regras obrigatórias e vinculantes, ou lei brandas. O arcabouço legal deve ser transparente e empoderar os consumidores. Para finalizar, retoma o debate sobre a responsabilidade sobre o conteúdo publicado questionando; se algo ilegal é publicado nas redes sociais quem deve responder legalmente? É o operador ou quem publicou? Quem criou o conteúdo ou quem o disseminou? Sendo assim, para garantir a liberdade de expressão as respostas à estas perguntas precisam ser transparentes e obviamente os operadores da rede possuem responsabilidade, afirma.

Por sua vez, o representante do Google, Allen Davidson, afirma que muitos experimentos estão em andamento, mas que eles sabem que as pessoas não utilizarão seus produtos se não tiverem confiança na empresa. Diz que eles não querem um mundo em que os provedores de mídias sociais sejam forçados e se tornarem *gatekeepers*. Já o representante do Facebook, Allen Davidson, diz que é um erro dizer que a Internet é um espaço onde não há regulação. Negócios que operam online estão sujeitos à uma vasta gama de leis, que envolvem desde a privacidade ao conteúdo ilegal, afirma.

Por sua vez, o representante da Unesco, Xianhong Hu, menciona um estudo realizado pela entidade em que se conclui que, com o crescimento do acesso à informação na Internet, a censura e o filtro de conteúdo são feitos não apenas pelas organizações governamentais, mas também por companhias privadas. Para o representante do terceiro setor, Vladimir Rudonovic, da *DiploFoundation*, os intermediários, sejam eles redes sociais, ou provedores de serviços da Internet,

devem permitir que as pessoas postem conteúdo sem revisão prévia. A revisão póstuma de conteúdo deve respeitar o devido processo legal e proteger contra maus usos. Regimes de notificação e retirada de conteúdo (*notice and take down*), antes de determinação judicial podem tornar-se sistemas de censura, prejudicando assim a liberdade de expressão.

Destacadas as principais intervenções deste ano, observa-se a consolidação do debate sobre remoção de conteúdo online, que está associado à questão da privacidade e proteção de dados pessoais devido ao fato de que, tanto as plataformas de conteúdo, como as autoridades, buscam identificar indivíduos que eventualmente burlem as regras. Trata-se de uma questão central que envolve diversas variáveis, que englobam tanto a liberdade de expressão, como a publicidade online. O ponto chave do debate é que cada vez mais as plataformas de conteúdo se tornarão os juízes e executores de suas próprias regras, determinando o que é ou não permitido, entretanto de acordo com valores comerciais.

Como se observará nos próximos anos, os critérios de priorização, a negligência com relação à determinados discursos de ódio e, ao mesmo tempo, a censura à determinados conteúdos será realizada a partir de regras pouco transparentes. Com isto, as plataformas de conteúdo exercem um controle privado sobre o que é veiculado na web. Ainda se deve considerar que a publicidade online é realizada de forma diversa se comparada à mídia tradicional. Não se trata apenas de propaganda direcionada, mas também de uma curadoria de conteúdo personalizado realizada a partir do mercado de dados pessoais.

É neste sentido que se identifica nas intervenções deste ano a necessidade do enquadramento da Internet em algum modelo de regulação. A sugestão dos participantes é o da radio fusão, ainda que a web funcione de forma bastante distinta. Há a necessidade de se estipular regras mínimas de atuação, que considerem os princípios democráticos da justiça, transparência, diversidade e pluralidade. Entretanto são outras variáveis que devem ser consideradas; os algoritmos de recomendação, ferramentas de auto completar e outros mecanismos que indicam o conteúdo, já que a forma de interação online é muito mais ativa do que nos meios de comunicação tradicionais. Neste sentido, observa-se que o debate sobre a responsabilização dos intermediários evoluiu com relação aos anos anteriores. Já não se questiona se possuem, ou não, responsabilidade, mas sim de que forma devem proceder diante da publicação de determinado conteúdo. Sobretudo quais são as regras aplicadas. O que se considera como impróprio?

Outra controvérsia central envolve a liberdade de expressão, o livre compartilhamento de informações e a proteção da propriedade intelectual. Os direitos autorais estão no centro da controvérsia sobre a livre fruição de conteúdo online, que incide na privacidade e proteção de dados pessoais devido aos conceitos de inimputabilidade e neutralidade de rede antes debatidos. A bandeira do combate à pirataria servirá de argumento para a consolidação do regime de notificação e retirada

de conteúdo. Por outro lado, a remoção de notícias falsas, discurso de ódio, dentre outros conteúdos não será tão efetiva.

Todas estas controvérsias serão aprofundadas nos debates dos anos posteriores. Realizadas estas considerações parte-se para a análise do ano seguinte, quando o Fórum foi realizado pela primeira vez no continente africano, em Nairóbi, no Quênia. Antes de mais nada, é importante indicar que o ano de 2011 é aquele em que a palavra "direitos" é menos mencionada nas sessões principais do Fórum. Das 162 sessões principais analisadas, apenas em seis delas o termo "direitos" não é evocado pelos participantes. Estas seis sessões em que a palavra "direitos" não possui nenhuma ocorrência aconteceram duas em 2007, e outras quatro em 2008. Sendo assim, pode-se afirmar que, de 2009 em diante, o termo "direitos" foi evocado pelos participantes em todas as sessões principais do Fórum. Totalizando três mil quinhentas e quarenta e três (3543) ocorrências o termo oscilou anualmente da seguinte forma:

Gráfico 3: Mobilização do termo "direitos" nas sessões principais do Fórum.

Fonte: Autora a partir de dados extraídos do site.

De imediato, percebe-se que, após 2011, os anos em que a palavra "direitos" foi menos mobilizada foram em 2014, quando há uma queda em todos os termos e em 2018, sendo que neste ano houve uma sessão principal com o termo direitos humanos no título. A hipótese desta queda será

explorada adiante. De forma contrária, observa-se que em 2013 e 2015 foram os anos em que o termo foi mais mobilizado.

Em 2011, durante a plenária "Segurança, abertura e privacidade", a palavra "segurança" foi mobilizada cento e quatorze (114) vezes, seguida por "privacidade" com setenta e oito (78) ocorrências, "direitos" com cinquenta e sete (57) e "liberdade" com trinta e nove (39). O termo "vigilância" é mobilizado sete vezes ao longo da atividade, representando mais do que o dobro de anos anteriores.

Ainda adotando o formato de plenária, a atividade contou novamente com a participação do consultor da ONU, Frank La Rue, que em suas considerações iniciais ressalta noção da Internet enquanto um espaço público. Por sua vez, Neelie Kroes, representante de organizações intergovernamentais, termina sua intervenção inicial destacando a Primavera Árabe e o enorme potencial da Internet em promover a democracia, a participação social e o fortalecimento dos direitos humanos.

Por sua vez, o representante da Microsoft, Heba Ranzy, retoma a retórica de que excessos de regras irão acabar com a criatividade do setor de tecnologia, mas reconhece que a ausência de normas tornaria a Internet um espaço para criminosos e ataques de negação de serviço (DDoS). Defende que os intermediários não sejam responsabilizados pela publicação de conteúdo ilegal gerado por terceiros.

Já a representante do terceiro setor, Christine Runnegar da *Internet Society*, enfatiza que a computação na nuvem apresenta vários riscos à privacidade. Destaca 1que os dados pessoais são cada vez mais utilizados para a categorização de perfis, em um processo em que as empresas estão "interrogando os consumidores". Ressalta que não existe a garantia de proteção à privacidade, e que deveria haver limitações aplicadas ao propósito dos dados coletados, por todos os tipos de entidades. Finaliza questionando quais seriam as condições para que o sistema de justiça obtenha acesso aos dados pessoais e se diz preocupada com a tendência de que agentes de aplicação da lei e garantia da segurança pública estejam sendo privatizados.

Em seguida, Xianhong Hu, da Unesco, ao reportar sobre uma atividade paralela, diz que o debate enfatizou que as mídias sociais são utilizadas tanto para a comunicação pessoal, como também para tratar de questões políticas, que não são abordadas pelas mídias tradicionais. Por outro lado, identifica riscos deste uso das redes sociais tais como; padrões éticos aplicados na criação de contas, a inadequação da proteção aos menores de idade, a privacidade dos cidadãos, a opacidade do tratamento de dados pessoais e, por fim, o filtro de conteúdo e a vigilância.

Quando o microfone é aberto ao público ocorre uma interessante polêmica. Um membro do parlamento do Reino Unido, Alun Michael, defende o governo de seu país, afirmando que não houve intervenção em termos de fechamento de redes sociais durante os protestos de agosto (entre 6 e 10

deste mês várias cidades inglesas tiveram protestos que resultaram na morte de cinco pessoas[85]). Para ele, o que ocorreu não foram atividades políticas e sim criminais.

Por sua vez, Johan Hallenborg, representante do governo sueco, diz que muitos países derrubam a Internet local em resposta à "legítimas aspirações do povo em fazer suas vozes serem ouvidas e clamarem por seus direitos". Declara que seu país é contrário à limitação do acesso à Internet, porque isso reduz o direito à liberdade de expressão e a livre associação. Finaliza indicando que os intermediários, sejam eles provedores de serviços ou outros, não deveriam ser responsabilizados pelo conteúdo gerado por terceiros.

A representante do terceiro setor, Katarzyna Szymielewicz, da *Panoptykon Foundation*, responde ao comentário do parlamentar britânico afirmando que ela não se referiu ao incidente em momento algum, mas que era um bom exemplo para se discutir sobre o papel dos provedores de serviços. Para ela, o argumento apresentado - de que determinados conteúdos são ilegais portanto não são necessárias novas proteções legais - é uma lógica que vai contra todo o conceito de sistema de justiça. Para ela, é papel da justiça decidir qual conteúdo é ilegal, ou não, e que estes limites são, por vezes, vagos. Finaliza indicando que os provedores de serviços possuem um papel muito importante em ajudar o sistema de justiça, mas que não podem substituí-lo. Para ela, colocar a responsabilidade nos intermediários enfraquece valores essenciais da democracia, o que não é bom nem para os negócios, nem para os cidadãos.

Em seguida, La Rue diz que concorda com a posição de Szymielewicz de que as medidas de segurança precisam ser definidas por lei. Para ele, os governos não podem interpretar de forma subjetiva as medidas de limitação, porque neste caso seriam decisões políticas. Sendo assim, defende que o Estado tem uma responsabilidade que não pode ser delegada. Destaca que é dever do judiciário implementar as leis, o que inclui inclusive a não privatização das responsabilidades do Estado. Na sequência, endossando as falas anteriores, a representante da Comissão da União Europeia afirma que os interesses privados não podem triunfar sobre os interesses públicos.

Durante a sessão, Vint Cerf, do Google, reconheceu que, se a empresa encriptasse todos os dados de seus usuários, não conseguiriam operar como uma companhia, já que não poderiam mirar os usuários em seus anúncios. Um participante da audiência rebate dizendo que isso demonstra que quando o modelo de negócio das empresas está em conflito com a necessidade de proteger os dados privados de seus consumidores, a privacidade é negligenciada. Outra intervenção do público é feita por Tom Wamalwa que ressalta que a Internet mudou ao longo dos anos e que seu propósito inicial de liberdade, abertura e compartilhamento já não são mais os mesmos.

---

[85] Entenda os tumultos no Reino Unido. Disponível em <http://g1.globo.com/mundo/noticia/2011/08/entenda-os-tumultos-no-reino-unido.html>. Acesso em 2/1/20.

Por sua vez, o representante do ministério de Telecomunicações e Mídia da Rússia, identificado apenas como Igor, enfatiza que as práticas atuais de governança da rede, impedem que os governos locais se responsabilizem sobre a estabilidade, a continuidade e a segurança das fontes de informação e da infraestrutura da Internet. Sua crítica é com relação à centralização da rede, antecipando o debate que surgiria com mais ênfase nos anos seguintes sobre a balcanização da Internet. Após quase três horas de debate a plenária é dada como encerrada.

A efervescência política do ano de 2011 se refletiu na atividade do Fórum com falas que enfatizaram o uso político das redes sociais, em eventos como a mencionada Primavera Árabe e os protestos no Reino Unido. Neste mesmo ano é deflagrado o movimento *Ocuppy Wall Street*, nos Estados Unidos, que questiona o sistema financeiro global, e os Indignados na Espanha, que realizaram uma série de protestos contra o sistema político do país (Castañeda, 2012). Além destes é relevante destacar ainda o movimento estudantil chileno, que neste ano protestou contra o sistema de ensino privatizado de seu país (Von Bülow e Ponte, 2015). Observa-se, portanto, um clima de otimismo com relação ao uso da web na organização política e no engajamento social, ainda que se reconheça o risco da vigilância realizada pelo Estado, ou pelas próprias plataformas.

Justamente quando aparentemente a web se consolidaria como instrumento para ampliar a participação política, a segunda fase do capitalismo de vigilância se consolida. Com a expansão da chamada computação na nuvem, que se refere à capacidade de armazenamento de dados em uma infraestrutura não local, cresce a preocupação com as dinâmicas de vigilância, mas também com a economia de dados. Importante notar que a própria computação na nuvem precede o fenômeno da *big data*. A computação móvel representa uma nova fonte de informações, que amplia a coleta de dados pessoais da computação pessoal para o mundo físico. Em paralelo, as plataformas de conteúdo testam filtros e novas formas de visualização. É em 2011, por exemplo, que o Facebook implementa a linha do tempo[86].

Diante da consolidação das redes sociais como principal forma de interação online, a controvérsia sobre o papel dos intermediários adquire novos elementos. As plataformas de conteúdo, que antes não queriam se responsabilizar pelo conteúdo publicado por terceiros, já adotam medidas muito pouco transparentes sobre suas práticas de gerenciamento. Retiram o que consideram inapropriado como por exemplo a nudez, mas mantém páginas racistas, misóginas e xenofóbicas. Com isto, determinam as regras sobre o que pode ou não ser veiculado a partir de critérios pouco transparentes e baseados em valores comerciais e não necessariamente princípios democráticos de

[86] How To Get your New Facebook Profile (Timeline). Disponível em http://www.techomag.com/how-to-get-your-new-facebook-timeline-before-the-released-date/. Acesso em 2/1/20.

pluralidade e diversidade na comunicação. Com isto, ferem a liberdade de expressão ao mesmo tempo em que falham em conter a disseminação de conteúdos ilegais, como o discurso de ódio, por exemplo.

Sobretudo, desenvolvem algoritmos de inteligência artificial para gerenciar estes filtros de conteúdo, colocando interações pessoais sob decisões tomadas por máquinas. A ausência de transparência sobre os critérios adotados por estes algoritmos não permite com que seja feita uma auditoria dos mesmos e indica que reproduzem padrões de discriminação racial e gênero em especial, mas também de renda a partir da categorização e criação de perfis de usuários.

É neste contexto que surge a controvérsia dos bancos de dados de perfis, utilizados para os mais diversos propósitos, da seleção para empregos, ao crédito, dentre outros. Os termos de uso determinam que as informações pessoais podem ser compartilhadas com "terceiros" o que permite a expansão do capitalismo de vigilância e a consolidação do mercado de dados pessoais.

Por fim, surge ainda de forma tímida a preocupação sobre a dependência dos Estados nação à infraestrutura da Internet, concentrada no norte global, em especial nos Estados Unidos. Justamente por isso, a China tem um controle interno da Internet no país, modelo reproduzido cada vez mais em outros países[87]. É neste contexto que surgem propostas de que estes dados sejam armazenados localmente, sob as leis dos países onde as informações são coletadas, de forma a proteger a privacidade dos cidadãos localmente.

Antes de prosseguir para a análise dos discursos do próximo ano é importante enfatizar que as controvérsias evoluem, tanto pela maturidade do debate, como também pelo próprio avanço tecnológico, em especial a mobilidade e a *big data*. É neste contexto que a questão da vigilância, praticamente ausente dos debates em anos anteriores, começa a ser colocada, principalmente por integrantes da sociedade civil.

Em 2012, o Fórum ocorreu em Baku, Azerbaijão, país localizado no sudeste asiático, que fez parte da União Soviética até 1991. A plenária "Segurança, abertura e privacidade" ocorreu dia 8 de novembro[88]. Na ocasião o termo "direitos" foi o mais mobilizado com oitenta e cinco (85) entradas, seguido por "segurança" com oitenta e quatro (84), "liberdade" com setenta e cinco (75) e "privacidade" com setenta e duas (72) ocorrências. Já o termo "vigilância" dobra com relação ao ano anterior, mas ainda com uma baixa ocorrência de quatorze (14) menções.

Dentre as considerações iniciais dos palestrantes, vale destacar a fala da representante do terceiro setor, Kirsty Hughes, que abordou diretamente a questão da vigilância em massa e a coleta indiscriminada de dados pessoais. Segundo ela, as pessoas tendem a realizar uma autocensura ao saber que estão sendo monitoradas, ao mesmo tempo que não sabem se estão conversando, debatendo

---

[87] Rússia mira modelo chinês e cria Internet própria. Disponível em < https://www.dw.com/pt-br/r%C3%BAssia-mira-modelo-chin%C3%AAs-e-cria-Internet-pr%C3%B3pria/a-48579585>. Acesso em 23/9/19.
[88] Disponível em < https://www.youtube.com/watch?v=KdSBmiHuMfs>. Acessado em 12/8/19.

e compartilhando informações em um espaço público, ou privado. Disse ainda que, inibir ou regular discursos de ódio, deve ser feito de uma forma limitada e que a regra geral que deve prevalecer é a liberdade de expressão.

Por sua vez, o representante do setor acadêmico Carlton Samuels, enfatizou que se a Internet é global sua segurança não deveria ser vista a partir de uma visão limitada, ou nacionalista. Para ele, o princípio diplomático da soberania westfaliana, que limita a soberania ao território, separando política interna da externa, não é o mais adequado para lidar com a Internet global. Já a representante parlamento Europeu, se diz uma política liberal, contra o excesso de regulamentação, mas defende a atualização das legislações levando em consideração os direitos humanos, a liberdade de competição e o livre comercio, a democracia e a segurança das pessoas.

Outra representante do terceiro setor, Eleonora Ravinovich, da *Association for Civil Rights*, da Argentina, ressaltou que o combate aos cibercrimes como a pirataria são ameaças para a abertura da Internet, a liberdade de expressão e o acesso à informação. Citou exemplos de legislações em tramitação em países da América Latina que dão muito poder policial de fiscalização da Internet. Mencionou ainda que, devido a tratados militares com os Estados Unidos, alguns países da região foram forçados a aprovar legislações contra a pirataria.

O advogado paquistanês Zahid Jamil, tratou diretamente da questão da vigilância ao citar o exemplo da blogueira feminista do Egito, Yara Salam que foi vigiada pelo governo devido à suas críticas[89]. Para ele, muitas pessoas se resignaram de se expressar online, referindo-se à autocensura.

Já Kristy Hughes, da ONG internacional *Index on Censorship*, comentou sobre o papel do anonimato e os desafios de defensores de direitos humanos em alguns países autoritários. Neste contexto, a representante do parlamento europeu, Neelie Kroes, ponderou que o que é lei em um país em termos de direitos e segurança das pessoas, pode significar coisas completamente diferentes em outros países onde ocorrem abusos das autoridades. Citou o próprio país sede do evento, o Azerbaijão, em que o estado de direito, os direitos humanos e a segurança são pontos que ainda precisam ser aprimorados. Para ela, as tecnologias são projetadas para propósitos específicos, às vezes com a finalidade de seguir e rastrear dissidentes, ou realizar vigilância em massa.

Com relação a isso, o representante do governo estadunidense, Christopher Painter, comenta que em determinadas situações é preciso preservar o direito das pessoas ao anonimato, a liberdade de expressão, mas que em outras situações é necessário que as pessoas se identifiquem e autentiquem suas operações, como em transações bancárias, por exemplo.

---

[89] Case History: Yara Sallam | Front Line Defenders. Disponível em < https://www.frontlinedefenders.org/en/case/case-history-yara-sallam >. Acesso em 2/2/20.

Após as falas iniciais o microfone é aberto para que pessoas reportem sobre outras atividades relacionadas ao tema de segurança, privacidade e abertura. O primeiro é realizado por representantes do projeto *Youth IGF Project*, criado para ampliar a participação de jovens nos debates sobre governança da Internet. Matthew Jackman e Nicola Douglas relatam que o anonimato foi um tema controverso, pois ao mesmo tempo em que pode ser positivo, empoderando pessoas que não teriam voz sem serem anônimas, pode ser utilizado para ofender outras pessoas.

De forma semelhante, outros representantes reportaram sobre o workshop sobre jovens combatendo o discurso de ódio, um projeto do Conselho da Europa, que aborda questões como o cyberbullying e ofensas à dignidade humana. Rui Gomes conta que algumas pessoas criticam o anonimato online porque acreditam que as pessoas tendem a dizer coisas que não diriam presencialmente. Com isso, algumas expressões passam a ser mais toleradas, inclusive algumas que abordam diretamente questões como nacionalidade e religião. Segundo ele, os participantes opinaram que este tipo de discurso não seria aceito em outros ambientes.

De volta aos comentários dos palestrantes, a representante do terceiro setor, Eleonora Rabinovich, defende que apenas o poder do Estado tem legitimidade de limitar a liberdade de expressão, para combater o incitamento ao ódio, segundo padrões internacionais de direitos humanos. Sobre este tema, Kirsty Hughes, também do terceiro setor, comenta que a religião e o discurso de ódio suscitam questões sobre identidade e liberdade de discussão, portanto, desafiam muitos pontos de vista e crenças. Complementa dizendo que a liberdade de expressão inclui o direito de não ser discriminado e a liberdade de crença.

Neste contexto, Rabinovich defende a proteção de minorias, mas argumenta que há evidencias que o bloqueio de conteúdo online ou offline não é a melhor solução. Ela explica que na América do Sul a liberdade de expressão é uma tradição muito forte e não se pode simplesmente banir determinados conteúdos ofensivos ou chocantes. Enfatiza que na Europa há mais tolerância na proibição de determinados tipos de discurso, como por exemplo a negação do holocausto. Por sua vez, o representante do governo do Egito, Sherif Hashem, invoca o princípio da proporcionalidade. Para ele há uma diferença entre a crítica e a tentativa de prejudicar outros, portanto, são temas que precisam ser abordados separadamente.

Outras pessoas voltam a reportar sobre atividades paralelas. Dentre eles, Andy Smith que falou sobre a atividade sobre aspectos da identidade digital. Segundo ele existe uma diferença significante entre privacidade e anonimato. Diz que o anonimato é a possibilidade de realizar ações sem deixar vestígios, o exercício da liberdade de expressão sem o temor das repercussões, o que denota, por outro lado, que as pessoas não podem ser responsabilizadas por seus atos. A privacidade significaria a habilidade de fornecer informações pessoais para aqueles autorizados pela lei, ou pela própria pessoa, que escolhe fornecer os dados segundo suas próprias prerrogativas. Por isso,

argumenta que a privacidade não prejudica a segurança na aplicação da lei, enquanto o anonimato pode fazê-lo. Relata que a identidade é utilizada como uma forma de moeda na Internet, as pessoas cedem informações pessoais para adquirir acesso a serviços. Finaliza dizendo que o tema da identidade digital será central na globalização da Internet.

Na sequência, Anja Kovacs reporta sobre o workshop cuja temática foi a tensão entre a aplicação da lei e uma Internet livre e aberta. Ela ressalta que o setor privado desempenha um papel central na aplicação da lei, ao criar seus próprios termos de uso. Estes contratos são vistos pelos participantes como constituições acidentais, no sentido de que são outro nível de regulação em que as pessoas precisam respeitar se querem se expressar livremente. Identificaram a privatização dos mecanismos de aplicação das leis e como os cidadãos possuem poucos recursos para contrapor a isso.

Em seguida, a palavra é passada para Malcolm Hutty, que reporta sobre o workshop sobre a proteção do Estado de Direito. Os participantes questionaram a privatização da aplicação da lei, em que os intermediários são cada vez mais responsabilizados por executar sanções sobre determinados conteúdos e comportamentos. Com o tempo restante restrito o moderador solicita que os palestrantes façam suas considerações finais, nas quais que repetem os argumentos já mobilizados. Após quase três horas de atividade a sessão é finalizada.

Antes de prosseguir na análise dos discursos sobre privacidade, direitos e democracia e seus argumentos mobilizados nesta sessão do Fórum é importante contextualizar o local em que o evento ocorre. Como bem mencionado por um dos integrantes da plenária, o Azerbaijão é governado sob um sistema de partido dominante, o Partido do Novo Azerbaijão, acusado por organizações internacionais por violações de direitos humanos, como perseguições à jornalistas e à integrantes da comunidade LGBT[90]. O presidente do país, Ilham Aliyev, está no poder desde 2003, sendo, portanto, considerado um país com regime autoritário por outros Estados Nação. Esta realidade se reflete na própria ocorrência da palavra direitos, a mais mobilizada pelos participantes durante as plenárias deste ano totalizando duzentas e sessenta e cinco (265) entradas.

Sendo assim, pode-se considerar que o tema dos direitos humanos se consolida nos debates sobre privacidade, segurança e abertura ocorridos nos últimos anos do Fórum de Governança da Internet. Por outro lado, argumenta-se o fato de que regimes autoritários não respeitam estes direitos, perseguindo dissidentes e opositores, tanto no mundo físico, como online. Sendo assim, se reconhece que a aplicação dos direitos humanos é assimétrica em diferentes países do mundo.

Este foi o ano em que o tema do anonimato foi mais mobilizado pelos participantes. Argumentos de que é necessário o anonimato para o exercício da liberdade de expressão, em especial em países autoritários, que perseguem críticos do governo, foram recorrentes. Por outro lado,

[90]Human Rights Watch. Disponível em https://www.hrw.org/europe/central-asia/azerbaijan. Acessado em 12/8/19.

ponderou-se que ele facilita a propagação de discurso de ódio. A controvérsia sobre os limites da liberdade de expressão foi colocada ainda na perspectiva da remoção de conteúdo e a limitação de linguagens ofensivas, às vezes necessárias para chamar a atenção do público para mudanças sociais. Neste contexto, a controvérsia sobre a responsabilidade dos intermediários é retomada a partir de uma crítica mais contundente com relação aos termos de uso e as sanções aplicadas pelas próprias plataformas a seus usuários, criando assim um sistema de justiça paralelo.

Por fim, o tema da vigilância aparece pela primeira vez na fala de um dos painelistas. Ela é tratada a partir do exercício da autocensura, ou seja, as pessoas reconhecem que ao serem vigiadas limitam sua liberdade de expressão. A questão explodiria no ano seguinte.

3.3 -As revelações de 2013 e o silêncio de 2014.

O ano de 2013 é um divisor de águas para o debate sobre privacidade online devido às revelações de Edward Snowden à Glenn Greenwald sobre o esquema de vigilância em massa exercido pela Agência Nacional de Segurança dos Estados Unidos, em parceria com as maiores empresas de tecnologia do mundo. O Fórum de Governança da Internet ocorre poucos meses depois das primeiras reportagens, que exibiram que o governo americano espionava desde a chanceler alemã Angel Merkel, até cidadãos comuns, armazenando um volume de dados pessoais que poderiam ser utilizados a qualquer tempo e para finalidades pouco transparentes.

Sendo assim, várias discussões do Fórum foram influenciadas por estas revelações, a começar pelo desmembramento da tradicional atividade sobre "Privacidade, Segurança e Abertura", que ocorria anualmente desde 2008. Dentre as oito atividades principais, a que os termos de pesquisa obtiveram mais ocorrência foi a sessão "Fazendo um balanço de questões emergentes; vigilância na Internet", ocorrida dia 25 de outubro[91], em Bali, na Indonésia (país que até 1998 era uma ditadura militar, apoiada pelos Estados Unidos).

Na ocasião, a palavra "privacidade" foi mobilizada quarenta e nove (49) vezes, "segurança" sessenta e oito (68) vezes, "direitos" cento e vinte e cinco (125) vezes, "liberdade" vinte e oito (28) vezes. O termo "vigilância" foi mencionado em oitenta e sete (87) ocasiões, representando sua maior ocorrência nas sessões principais do Fórum. De fato, neste ano se observa um salto na mobilização da palavra, conforme se verifica no gráfico de sua evolução anual.

[91] Fazendo um balanço de questões emergentes; vigilância na Internet. Disponível em https://www.youtube.com/watch?reload=9&v=jIswrxWSiF4. Acessado em 12/8/19.

Gráfico 4: Mobilização da palavra "vigilância" nas sessões principais do Fórum.

Fonte: Autora a partir de dados extraídos do site.

Os dados indicam que, nos primeiros anos do Fórum, o termo "vigilância" praticamente não era abordado nas sessões principais. A palavra aparece de forma discreta ao longo dos anos totalizando apenas trezentas e cinquenta e seis (356) ocorrências. Somente em 2013, são cento e setenta e cinco (175) vezes, ou seja, mais da metade do número total. O salto gráfico é o mais alto dentre todos os termos pesquisados na análise quantitativa.

O que contribui com esse aumento é outra sessão principal, intitulada "Direitos humanos, liberdade de expressão e a livre circulação de informação na Internet", em que o termo "vigilância" é mobilizado sessenta e quatro (64) vezes. Observa-se que, pela primeira vez, o tema da liberdade de expressão é tratado diretamente nas sessões principais do Fórum de Governança da Internet.

A atividade de 2013, sobre vigilância na Internet, adotou o formato de painel, com menções a atividades paralelas que abordaram questões de privacidade e segurança. Conforme se observará nas próximas páginas, trata-se de uma das atividades mais polêmicas ocorridas durante o Fórum. As controvérsias surgem devido às recentes revelações de Edward Snowden sobre o aparato de vigilância implementado pela agência de segurança dos Estados Unidos. Além disso, o debate contou com a presença de um representante do governo estadunidense - Scott Busby - e outro do Google - Ross LaJeunesse, que foram questionados tanto por outros palestrantes, como pelo público.

A atividade contou com três moderadores; Markus Kummer, do ICANN, Anne-Rachel Inne, da agência técnica *AfriNIC* e Jovan Kurbalija, da ONG suíça *DiploFoundation*. Dentre os palestrantes havia ainda Johann Hallenborg, do governo da Suécia, Jari Arkko, da *Internet Engineering Task Force* (IETF) e Joana Varon, da ONG brasileira *Coding Rights.*

Após apresentar os temas do debate, o moderador Jovan passa a palavra para os comentários iniciais de cada um dos palestrantes. O primeiro a discursar é Scott Busby, do governo estadunidense, que faz uma fala defensiva, protocolar e retórica. Em resumo, ele diz que os Estados Unidos comparecem anualmente ao Fórum defendendo uma Internet aberta, segura e interoperável e reconhece a importância do tema da vigilância para a comunidade internacional. Admite que existem preocupações causadas pelos recentes relatórios sobre a suposta prática de inteligência de seu país e menciona o então presidente Obama diversas vezes. Afirma que todos os países do mundo coletam dados de inteligência, que identificam como ameaças à segurança nacional. Atesta que as práticas de seu país respeitam os direitos humanos e princípios democráticos.

Prossegue dizendo que é normal não comentar sobre alegações envolvendo atividades de inteligência, ainda assim, ressalta que seu país não usa os dados coletados com o propósito de reprimir cidadãos de quaisquer países e por quaisquer motivos, incluindo suas crenças políticas, religiosas ou outras. Quota o presidente Obama ao afirmar que o país não está interessado em espionar pessoas comuns. Finaliza condenando governos que prendem, ou intimidam oponentes.

Em seguida, o microfone segue para Ross LaJeunesse, do Google, que inicia esclarecendo algumas questões. A primeira delas é que a empresa não fornece acesso direito a seus dados, servidores e infraestrutura para nenhum governo. Afirma que não aceitam requisições gerais de governos, ainda que estejam sujeitos às leis. Portanto, quando algum governo solicita acesso as informações de seus usuários, o time de advogados do Google analisa as requisições avaliando se são válidas, legais, seguem o devido processo legal e são limitadas em termos de escopo. Atesta que muitas vezes se recusam a fornecer os dados solicitados.

Enfatiza que seria mais fácil para o Google o simplesmente atender os governos e fornecer os dados dos usuários, mas que não operam assim, pois se a empresa não tiver a confiança dos usuários as pessoas não vão utilizar seus produtos. Finaliza reiterando o que o representante do governo americano disse sobre países em que jornalistas são açoitados, ativistas são assassinados e blogueiros são presos. Afirma que está aberto a discutir a suposta hipocrisia do governo americano e outros países ocidentais, mas que eles não devem ser atacados, pois desempenham um importante papel de apoio ao modelo multissetorial de governança da Internet.

Na sequência, o representante da comunidade técnica, Jari Arkko, reconhece que os relatórios recentes sobre o monitoramento em larga escala são preocupantes. Ainda assim, pondera que a interceptação de determinados indivíduos e as atividades de inteligência são bem conhecidas. Diz

ainda que no âmbito da *Internet Engineering Task Force* (IETF), desde 1994, se reconhece a criptografia como uma importante ferramenta para proteger a privacidade das comunicações. Finaliza destacando a importância da comunidade *open source* e que suas soluções são uteis para reforçar a confiabilidade das ferramentas.

O representante do governo sueco discursa sobre princípios democráticos, direitos e liberdades e o papel do Estado em garanti-los. Destaca que a legislação de seu país faz uma distinção entre a vigilância de comunicação eletrônica e coleta de informações de inteligência. Para ele, a diferença é essencial, já que os objetivos operacionais de cada uma delas também se diferem. Finaliza citando o ministro Carl Bildt, que na Conferência de Seul sobre o Ciberespaço, ocorrida no mês anterior, destacou sete princípios para realizar a vigilância de comunicações eletrônicas; legalidade, legítimo objetivo, necessidade e adequação, proporcionalidade, autorização judicial, transparência e supervisão pública.

Por sua vez, Joana Varon, representante do terceiro setor do Brasil, destaca que as revelações sobre os programas de vigilância em massa das agências de segurança dos Estados Unidos demonstraram que se realiza uma vigilância entre fronteiras sem precedentes em termos de alcance e escopo. Para ela, o argumento de segurança nacional e prevenção de ameaças não justifica o escopo da vigilância realizada, que inclusive grampeou presidentes de países como o Brasil, considerados como nações amigas.

Afirma ainda que não importa se os dados foram utilizados ou não, pois simplesmente sua coleta já representa um completo desrespeito ao direito à privacidade dos cidadãos de todo o mundo, e de convenções internacionais de direitos humanos. Em uma crítica direta aos representantes do governo americano e do Google, ela solicita que analisem os Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações assinados por mais de 280 organizações internacionais[92].

Após outras intervenções que reforçam aspectos já mencionados, o debate é aberto para duas perguntas remotas. A primeira é dirigida ao representante do governo dos Estados Unidos e a segunda para o do Google; “a defesa dos interesses da política externa dos EUA inclui a vigilância dos telefones dos chefes de governo, dos países que são amigos dos EUA?” e “o que o Google pretende fazer para restaurar a confiança das pessoas?”.

Dentre as intervenções presenciais a que apresenta novos elementos é realizada por Bertrand de la Chapelle, da comunidade técnica da França. Para ele, as revelações de Snowden colocaram em pauta a noção de soberania de dados, que requer que os dados coletados estejam associados ao

[92] Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações. https://necessaryandproportionate.org/pt/princ%C3%ADpios-internacionais-sobre-aplica%C3%A7%C3%A3o-dos-direitos-humanos-na-vigil%C3%A2ncia-das-comunica%C3%A7%C3%B5es. Acessado em 12/8/19.

território de seus cidadãos. Enfatiza que ações realizadas em determinado território impactam outros Estados nação devido à arquitetura transfronteiriça da Internet. Para ele, isto é um desafio já que o sistema internacional é baseado na separação de soberanias, que seguem o princípio de não intervenção. Destaca que a implementação de uma arquitetura de rede que retenha os dados em territórios específicos pode representar uma violação da privacidade ainda maior.

Por sua vez, Jan Malinowski, do Conselho da Europa, ressalta que desde a década de 1970 a Corte Europeia de Direitos Humanos deixou claro que um sistema de vigilância em massa pode debilitar, ou até mesmo destruir democracias sob o manto de protegê-las. Com relação ao caso Snowden, ele diz que o Conselho se preocupa com denunciantes (*whistleblowers*) e que estas pessoas, que revelam informações de interesse público, devem ser protegidas.

Outra crítica direta sobre o esquema de vigilância em massa revelado por Snowden é realizada por Ren Yishengm, que afirma que a delegação chinesa está surpresa e preocupada com o fato de que há uma vigilância em massa, que infringe a soberania, os interesses nacionais e a privacidade de pessoas de outros países. Por sua vez, Subi Chaturvedi, professora universitária da Índia, questiona qual o propósito, por quem, e por quanto tempo a os dados coletados pelos governos serão mantidos. Finaliza afirmando que democracia não é o mesmo que multisetorialíssimo e que é necessário reforçar estes sistemas.

Antes da participação da próxima pessoa da audiência, o moderador Kurbalija diz que tem uma questão direcionada ao representante estadunidense Scott Busby. Se diz satisfeito em saber que o governo americano mudou o tom de suas declarações, mas que no centro do debate há um homem chamado Snowden a quem o presidente Obama se referiu como traidor. Pergunta se ele mantém esta posição, ou se ela também se alterou.

Outra intervenção crítica é feita por Jimmy Schulz, ex membro do parlamento alemão, que reitera que a questão da vigilância não é nenhuma novidade. Faz uma pergunta direcionada ao Google, cujo representante afirmou que a empresa não fornecia acesso direto aos dados dos usuários; "existe acesso indireto? Vocês são forçados por alguma lei a não nos dizer tudo sobre as interceptações legais?". Prossegue se dirigindo agora ao representante do governo americano. Ele diz que Keith Alexander, general que à época era diretor da Agência Nacional de Segurança, afirmou que as pessoas que utilizam criptografia são tratadas como terroristas em potencial. "Você acha que sou um terrorista em potencial?" questiona.

Já Everton Lucero, integrante do governo brasileiro, questiona se a violação da privacidade de milhões de brasileiros e de empresas foi feita em nome da segurança nacional dos Estados Unidos. "Isto significa que existe uma suspeita de que cidadãos, autoridades e empresas brasileiras estão de alguma forma envolvidas com o terrorismo, ou alguma atividade que possa colocar em risco a segurança nacional de outros países", pergunta.

A próxima intervenção é do advogado Megi Margiyono. Ele questiona sobre como manter a Internet livre e aberta, à despeito das atividades de vigilância. Afirma que a liberdade de expressão nos Estados Unidos é "o direito mais importante", pois é protegido pela primeira emenda da constituição do país. Por outro lado, não está claro se a privacidade está protegida pela constituição. De forma contrária, para os países europeus, a privacidade é muito importante e existem determinadas limitações em sua aplicação. Na Ásia, por sua vez, a privacidade e a liberdade de expressão não são direitos consolidados e protegidos. Finaliza citando um relatório que aponta que tecnologias de vigilância são utilizadas para monitorar jornalistas em países como Emirados Árabes e que nada garante que o próprio governo da Indonésia, onde ocorre o Fórum, não esteja utilizando estas tecnologias para monitorar as atividades da oposição durante as eleições.

Mais adiante, Mike Gurstein, de uma ONG do Canadá, menciona o uso de drones para enfatizar que estamos enfrentando um problema mais grave que a simples vigilância. Para ele, estamos lidando com o uso potencial da intervenção ativa e direta de forma perigosa em aspectos do nosso dia a dia, incluindo transações bancárias, dados de saúde, as comunicações interpessoais. John Laprise, historiador e professor na Universidade de Northwestern, dos Estados Unidos, se diz perplexo que muitos Estados estejam surpresos com o escopo da vigilância realizada pela Agência Nacional de Segurança de seu país. Para ele, as pessoas deveriam olhar para as entidades de inteligência de seus próprios países, porque elas estão demonstrando que são incompetentes, ou não estão dizendo nada, o que as torna culpadas de conluio.

Outras intervenções do público são realizadas. Dentre elas Andres Azpurua, da Venezuela e integrante do *Internet Society*, que pondera que a vigilância em massa é realizada tanto por governos de grandes países como de pequenos. No caso destes últimos os controles e fiscalizações são ainda mais fracos do que o caso em discussão dos Estados Unidos. Ressalta que, em países como a Venezuela, a tecnologia de vigilância não é proveniente da indústria local, mas importada de nações desenvolvidas, que possuem indústrias de tecnologia mais fortes, em uma referência direta ao colonialismo digital. Neste contexto, o moderador Kurbalija comenta que os contratos entre os provedores de tecnologia e os governos deveriam prever que as tecnologias só serão utilizadas para propósitos legítimos.

Em seguida, os panelistas buscam responder aos questionamentos do público. O primeiro a falar é o representante do governo americano que, de imediato, reconhece que não poderá replicar todos questionamentos colocados. A parte a retórica defensiva, ele explica que o conceito de privacidade é posterior à constituição americana, mas que a suprema corte do país interpretou que ela cobre este direito. Sobre a Agência Nacional de Segurança de seu país ser um Estado dentro de um Estado, ele relembra que as atividades da agência estão sujeitas à revisão judicial e legislativa.

Em seguida, o representante do Google comenta sobre o questionamento de acesso direito e indireto, negando que a empresa forneça acesso à sua infraestrutura. Enfatiza que a computação na nuvem é muito mais segura que modelos alternativos, caracterizados por soberania de dados, ou dados localizados. Finaliza dizendo que não está trivializando as revelações sobre a vigilância dos Estados Unidos, mas enfatizando que não se trata de uma questão exclusiva deste país.

Posteriormente, Hallenborg, do governo sueco, aponta que são temas pouco regulados e que a lei de seu país não diferencia os cidadãos locais dos estrangeiros. A lei sueca reconhece a privacidade enquanto um direito de cidadãos suecos e não suecos.

Na sequência, Joana Varon, da ONG brasileira, volta a questionar o representante do governo americano, desta vez sobre os denunciantes, citando que as penalidades aplicadas a eles são cada vez piores. Cita o caso de Chelsea Manning, que vazou documentos do governo e está presa. Para ela, estas pessoas vivem em um dilema entre se tornarem traidores de suas nações e prover importantes informações ao mundo.

Ocorre uma nova tensão quando o representante da delegação chinesa Ren Yisheng pede a palavra novamente para dizer que o representante americano não foi sensível à sua intervenção. Afirma que os chineses conhecem as condições de direitos humanos de seu país e que outras nações não têm o direito de comentar sobre isso. Reforça que os chineses exercem sua liberdade de expressão, mas que as leis locais não permitem que se divulguem informações que podem colocar a segurança nacional em risco, tampouco notícias falsas. Pouco depois, a moderação faz alguns comentários e encerra o debate de quase três horas de duração.

A primeira observação com relação ao debate de 2013 é a participação do público tanto presencialmente, como remotamente. Foram cerca de trinta intervenções, algumas inclusive bastante incisivas diante das revelações de Snowden sobre a vigilância em massa realizada pela Agência Nacional de Segurança dos Estados Unidos. É possível notar nas falas iniciais, tanto do representante do governo dos Estados Unidos, como do representante do Google, uma tentativa de deslocar o foco do debate do recente escândalo apontando para países que utilizam a vigilância, mas violam direitos humanos e ferem a liberdade de expressão de forma mais autoritária.

Neste contexto, a principal controvérsia não é sobre a vigilância, ou atividades de inteligência em si, mas a escala e proporção com que são realizadas na passagem do modelo analógico para o digital. De fato, uma das intervenções da plateia é justamente neste sentido ao destacar que os governos que se dizem surpresos pelo aparato de vigilância dos Estados Unidos, ou são incompetentes, ou culpados de conluio.

O debate deste ano ficou em torno das revelações sobre vigilância, não apresentando grandes novas controvérsias com relação aos anos anteriores. Dentre as questões levantadas, é preciso ressaltar o colonialismo digital exercido por meio das tecnologias de vigilância, quando países

importam sistemas de controle, ou servem como teste para o desenvolvimento de novas técnicas de vigilância. Há uma assimetria em termos da possibilidade do exercício dos direitos humanos entre os países, e as empresas exploram estas lacunas. Esta desigualdade representa uma das principais controvérsias em torno do debate sobre privacidade e proteção de dados pessoais, principalmente diante do fato de que a União Europeia cria dois tipos de cidadãos a partir do Regulamento Geral de Proteção de Dados, ao proteger apenas aqueles nascidos no bloco. O restante dos cidadãos não apenas tem seus direitos suprimidos, como também se tornam alvo de tecnologias experimentais, que envolvem biometria, manipulação de DNA, reconhecimento facial, dentre outras, cada vez mais avançadas e pouco transparentes com relação à sua forma de funcionamento. É neste contexto que é preciso reconhecer que os direitos humanos, ainda que universais, não são implementados de forma equânime entre os Estados.

Dito isso, é importante destacar a intervenção do representante do governo sueco que explica que a legislação de seu país faz uma distinção entre a vigilância de comunicação eletrônica e coleta de informações de inteligência, já que são dados coletados com objetivos diferentes. Importante notar que, segundo ele, as leis de seu país não diferenciam cidadãos locais dos estrangeiros, reconhecendo a privacidade como um direito independentemente da nacionalidade. Ele enfatiza ainda sete princípios que devem ser levados em conta quando se realiza a vigilância de comunicações eletrônicas, a saber; legalidade, legítimo objetivo, necessidade e adequação, proporcionalidade, autorização judicial, transparência e supervisão pública.

Ainda no contexto das revelações de Snowden, uma controvérsia que surge neste ano é com relação à soberania de dados. Trata-se do armazenamento local das informações dos cidadãos de determinados países. Nessa lógica, empresas americanas que atuam no Brasil, por exemplo, deveriam manter servidores com as informações coletadas em território nacional dentro da fronteira brasileira e não apenas na "nuvem", ou seja, em parques tecnológicos de outros países. Longe de esgotar esta controvérsia, que envolve tanto o colonialismo de dados como a capacidade das empresas em impor determinadas legislações locais, o fato é que esse tipo de exigência pode enfraquecer ainda mais a segurança da informação, já que alguns países possuem uma legislação frágil sobre proteção de dados pessoais.

Outro ponto de destaque que havia surgido de forma tímida em anos anteriores é a criptografia. O representante da comunidade técnica diz que uma das principais entidades de segurança da Internet o IETF, reconhece, desde 1994, a criptografia como uma importante ferramenta para proteger a privacidade das comunicações. Por outro lado, uma intervenção da plateia indica que para algumas agencias de segurança as pessoas que utilizam estas técnicas são vistas como terroristas em potencial.

Dentre as controvérsias surge o debate sobre o papel dos denunciantes (*whistleblowers)*. Há um reconhecimento de que estas pessoas que revelam informações de interesse público deveriam ser

protegidas. Neste contexto é importante enfatizar que Chelsea Manning, que vazou documentos do governo americano ao *Wikileaks*, está presa há quase uma década. O mesmo destino de Julian Assange, que foi detido em 2019, após anos de refúgio na embaixada equatoriana na Inglaterra. O próprio Snowden segue em exílio na Rússia. Portanto, o padrão de tratamento de denunciantes, mesmo em países com democracias liberais, como Estados Unidos, é o encarceramento.

Um debate importante que surge neste ano, ainda que de forma tímida, é sobre os limites do modelo de governança e sua diferença da democracia liberal. Trata-se de uma questão central da discussão, pois os princípios de boa governança e de multisetorialíssimo são bem diferentes daqueles das democracias, ainda que limitadas ao modelo liberal e representativo. Existem semelhantes, como a pluralidade de atores, a consideração sobre benefícios mútuos, a própria transparência do Estado. Entretanto, as democracias partem da igualdade e do estabelecimento de um Estado de Direito. Já a governança – conceito este proveniente da área de administração – tem um propósito essencialmente econômico, ainda que possa levar em consideração a equidade dos atores envolvidos.

Realizados estes destaques, é preciso enfatizar que a plenária de 2013 torna central o debate sobre vigilância, apontando para a necessidade da proteção de dados e privacidade. Por outro lado, o ano seguinte, 2014, retrata a tendência oposta. Segundo os dados quantitativos levantados a partir das sessões principais do Fórum de Governança da Internet, 2014 foi o ano em que todos os termos pesquisados – privacidade, direitos, segurança, liberdade e vigilância – tiveram menor recorrência.

Em 2014, nona edição do Fórum ocorreu em Istambul, na Turquia entre os dias 2 e 5 de setembro. Dentre as quatorze sessões principais do evento este foi o primeiro e único ano em que os temas de segurança e privacidade não estavam presentes. As sessões principais trataram de temas recorrentes como o desenvolvimento e acesso, mas também de aspectos bem direcionados como a neutralidade de rede, a evolução do ecossistema da Internet e o futuro do Fórum.

Dentre as atividades principais a palavra “privacidade” é mobilizada apenas doze vezes na sessão de microfone aberto, no último dia do evento. Na ocasião o termo “segurança” foi mobilizado apenas oito vezes, “vigilância” cinco e “direitos” em onze ocasiões. Diante dos dados, as atividades principais de 2014 não indicaram relevância de uma análise qualitativa conforme foi realizado em trilhas que abordaram privacidade, segurança ou vigilância, nos anos anteriores e posteriores.

O silêncio de 2014 com relação ao debate sobre privacidade, proteção de dados pessoais, vigilância e a própria segurança representa a indisposição gerada pelas revelações de Snowden no ano anterior. É como se a realidade dos fatos tivesse sido incorporada e não houvesse alternativa ao capitalismo de vigilância, já que seria necessário transformar o modelo de negócios das grandes empresas de tecnologia para enfrentar a questão.

Por fim, antes de prosseguir para a análise dos próximos anos apresenta-se a evolução do termo "segurança" nas sessões principais do Fórum de Governança da Internet. A palavra foi encontrada três mil e quarenta e nove vezes (3049) vezes e varia da seguinte forma ao longo dos anos.

Gráfico 5: Mobilização do termo "segurança" nas sessões principais do Fórum.

Fonte: Autora a partir de dados extraídos do site.

Entre 2006 e 2019, o termo "segurança" só não foi mencionado em seis das cento e sessenta e duas (162) sessões principais analisadas. A queda de 2014, verificada junto aos outros termos, se dá em parte devido ao fato de que neste ano nenhuma das sessões principais contou com a tradicional trilha de segurança, tópico presente em todos anos anteriores. O mesmo pode ser dito com relação aos anos de 2016 e 2019 que não contaram com o tema de segurança em nenhuma de suas principais sessões.

Já a busca pela palavra "cibersegurança" resultou em oitocentas e setenta e sete (877) entradas. A sessão em que o termo cibersegurança mais aparece – com cento e sessenta e três (163) menções – é a de tópicos emergentes do ano de 2007. Por sua vez, a soma dos termos "segurança" e "cibersegurança" totalizam três mil novecentos e vinte e seis vezes (3926) menções, superando, todos os termos buscados, inclusive a palavra "diretos" que obteve três mil quinhentos e quarenta e três (3543) ocorrências.

Portanto, os dados indicam que o tema da segurança foi o mais mobilizado nas sessões principais do Fórum de Governança da Internet ao longo dos anos. Estas informações indicam a tendência de que há uma preocupação maior com segurança do que com os próprios direitos humanos, tão estimulados e invocados pelos participantes.

3.4 – Anos finais; 2015 a 2019.

A décima edição do Fórum de Governança da Internet ocorreu em João Pessoa, entre 10 e 13 de novembro, tornando o Brasil o único país do mundo a sediar o evento mais de uma vez. Dentre as onze atividades principais do Fórum de 2015, aquela em que a palavra "privacidade" obteve maior incidência foi a de "Direitos Humanos na Internet", com cinquenta (50) ocorrências. Nesta sessão a palavra "direitos" foi mobilizada cento e dezessete vezes (117), "segurança" dezessete (17), "vigilância" dez (10) e "liberdade" por cinquenta e seis vezes (56).

O tema da segurança retorna às atividades principais na trilha intitulada "Melhorando a cibersegurança e construindo confiança digital". Na ocasião, o termo "privacidade" obteve apenas seis (6) ocorrências. Portanto, seguindo a metodologia adotada, analisou-se o conteúdo da primeira atividade, em que a palavra "privacidade" foi mais mobilizada.

A sessão adotou o formato de mesa redonda. Dentre as considerações iniciais, destaca-se a fala de Frank La Rue, consultor da ONU, com presença recorrente no Fórum. Ele enfatizou a preocupação com o aumento do discurso de ódio, em especial durante campanhas eleitorais. Questionou a responsabilidade das corporações na venda de suas tecnologias; são comercializadas para Estados autoritários? Para ele, essa é uma grande preocupação.

Em seguida, o Professor Joe Canatacci, relator especial da ONU sobre direito à privacidade na era digital, destaca que a privacidade é condição para o exercício de outro direito; o direito à personalidade, que se refere ao direito de cada pessoa desenvolver sua personalidade de forma livre e desimpedida.

Por sua vez, o representante do setor privado, Ebele Okobi do Google enfatiza, a importância da auto regulação, mas também pondera que determinadas decisões cabem ao judiciário, ou outras instituições governamentais. Finaliza dizendo que o setor privado não quer ser aquele que decide o que deveria ser publicado ou não na Internet.

A jornalista indiana Bishakha Datta cita em sua fala uma pesquisa realizada junto a ativistas em que 51% deles disseram que receberam mensagens violentas, ou ameaçadoras, contendo intimidações. Para ela, as plataformas que removem conteúdo online exercem uma censura privada.

Questiona como podemos defender o direito à todas as formas de expressão, incluindo aquelas que são estigmatizadas? Como uma expressão de um usuário pode silenciar outros?

Por sua vez, Luis Garcia, do México, ressalta que muitas vezes a privacidade não é apenas violada, como também negada em agendas como, por exemplo, a de cibersegurança. Cita o exemplo de seu país, em que a legislação sobre cibercrimes dá muito poder de punição às autoridades. Menciona um relatório das Nações Unidas que indica que o país passa por uma grave crise de direitos humanos, com ocorrências de desaparecimentos, torturas e assassinatos, que afetam diretamente determinados grupos como, por exemplo, jornalistas. Finaliza dizendo que, quando algumas agendas como a de cibersegurança tentam colocar a privacidade, ou a criptografia, em contraste com a segurança deve-se considerar que em determinados países a linha entre o governo e o crime organizado é geralmente muito tênue. Neste contexto, o moderador comenta que se deve ter cuidado em deixar a responsabilidade por resguardar os direitos humanos apenas para o Estado. Para ele, o próprio mercado que opera na Internet deve se responsabilizar pelo respeito aos direitos humanos.

Dentre as intervenções relevantes da audiência destaca-se a de Beatriz Costa Barbosa, que enfatiza a questão da responsabilidade dos intermediários. Destaca que alguns Estados deixam as plataformas à cargo de determinadas decisões, renunciando a seu papel regulador. Por outro lado, diz que existem inúmeros exemplos em que estas plataformas afirmaram que alguns discursos de ódio, algumas violações de direitos humanos, não vão contra seus princípios, portanto deixam este tipo de conteúdo online. Finaliza questionando como se pode prevenir que estas violações de direitos continuem. Em sua opinião deve-se fortalecer as regras aos intermediários nesses processos.

Outro comentário relevante do público é realizado por Maarten Botterman, do ICANN. Para ele, a Internet das coisas (IoT) irá transformar a realidade atual, já que a *big data* representa uma grande mudança, o que coloca em discussão muitos aspectos da privacidade. Afirma que a proteção da privacidade é uma questão de dignidade humana. Nessa mesma linha, outro participante enfatiza que a com Internet das coisas, os dados estarão em todos os lugares e que a coleta de dados é inevitável, já que existem cada vez mais fontes de informação.

Neste contexto, outro participante enfatiza que algumas práticas de gerenciamento de dados são mais lucrativas que outras. Deve-se questionar se esses lucros são permitidos por lei, ou não. Diz ainda que a neutralidade de rede envolve obrigações de privacidade, já que a análise e a inspeção de pacotes frequentemente realizada no gerenciamento de dados pode ter sérias consequências para a privacidade.

Em outra intervenção, um participante comenta que existe uma preocupação sobre os usos possíveis dos dados no futuro. Destaca que o argumento das empresas é de que eles querem coletar todos os dados possíveis, que depois irão pensar sobre o que fazer com estas informações e que se

regulações interferirem neste modelo irão acabar com a inovação. Para ele não se trata desta dicotomia. Na sua opinião é possível inovar e se comprometer a identificar qual será o uso dos dados.

Após outras intervenções do público, La Rue faz as considerações finais do painel. Ele se diz satisfeito que após anos de debate os direitos humanos sejam o padrão de discussão (embora, como se observou a segurança seja mais mobilizada nos discursos das sessões principais do Fórum). Finaliza destacando que não se sabe o que estão fazendo nem que tecnologias são utilizadas, que sistemas de vigilância são vendidos para regimes autoritários, que perseguem jornalistas. Diz que há uma responsabilidade mútua entre a sociedade civil e as corporações no sentido de resolver estas questões. Em seguida a atividade é encerrada.

A sessão de 2015 retoma algumas controvérsias surgidas nos anos anteriores, como os limites entre discurso de ódio e liberdade de expressão, a responsabilidade dos intermediários, os modelos regulatórios, os filtros de conteúdo, dentre outras questões. Por outro lado, observa-se por parte dos panelistas um discurso mais conciliador e menos polêmico se comparado à outras edições. Por fim, nota-se a questão da segurança em termos de infraestrutura técnica é retomada nas sessões principais do Fórum, o que não ocorre com o tema da privacidade, que foi título das atividades principais nos anos anteriores.

Uma novidade nos discursos é a colocação do relator da ONU sobre a privacidade enquanto condição para o desenvolvimento da personalidade. Trata-se da noção moderna de intimidade, em que o retiro e o isolamento funcionam como oportunidade para o desenvolvimento pessoal. Estar livre dos mais variados tipos de coerção para o desenvolvimento da própria personalidade seria, portanto, um direito humano. A função da privacidade no mundo contemporâneo estaria associada ao desenvolvimento dos próprios sujeitos, ou o direito a si mesmo (*right to the self*). Neste sentido é interessante observar como a privacidade é elevada como um direito humano, ao mesmo tempo em que é renunciada em troca de serviços e aplicativos digitais.

A controvérsia entre os limites da liberdade de expressão e o discurso de ódio é retomada com ênfase neste ano. É reconhecido o fato de que certos discursos variam de acordo com países e culturas, sendo inaceitáveis em determinados locais, e mais tolerados em outros. Sob o guarda-chuva deste debate é retomada a questão da responsabilidade das plataformas sobre o conteúdo veiculado. Trata-se de uma censura privada, praticada pelas plataformas de acordo com as regras estabelecidas em seus próprios termos de uso, que não necessariamente priorizam a liberdade de expressão, ou outros valores democráticos, como a diversidade e pluralidade de discursos. Ao retirar determinado conteúdo do ar, e permitir outros, as plataformas tomam decisões que impactam a opinião pública. Como algumas plataformas de conteúdo permitem a veiculação de discursos misóginos e proíbem a nudez em casos de amamentação?

Uma nova controvérsia com relação à responsabilidade dos intermediários surge no questionamento sobre seus clientes. As empresas comercializam suas tecnologias para Estados autoritários, ou para agendas que dão ênfase excessiva à cibersegurança em detrimento dos direitos humanos? Este mesmo problema se apresenta no contexto das campanhas eleitorais. Qual a proveniência dos recursos dos anúncios políticos veiculados online? Eles divulgam que são pagos, como a propaganda no rádio e tv? Ocorre que, como dito, algumas práticas de gerenciamento de dados são mais lucrativas que outras. O mercado de dados está inclusive pensando nos usos futuros possíveis destas informações, como pondera outro participante.

Outra controvérsia retomada no debate é sobre a neutralidade de rede, que incide diretamente no exercício da privacidade, pois a verificação do conteúdo dos pacotes de dados que trafegam sobre a Internet indica o tipo de conteúdo que cada pessoa consome online. Importante destacar que na lei brasileira do Marco Civil da Internet ela é protegida, mas por outro lado ainda é uma questão em aberto nos Estados Unidos, o que tende a impactar outros países do mundo. O tema é tratado pelos congressistas do país, que em 2019, reviram uma decisão para a retomada deste princípio com vistas a garantir a igualdade no tráfego de dados[93].

Inclusive, este argumento, sobre decisões regionais que impactam diferentes países do mundo, é articulado pelos participantes, em crítica sobre o colonialismo digital. Seja ele realizado pela exportação de tecnologias de vigilância, ou até mesmo por imposição de protocolos técnicos, o fato relevante é que os países em desenvolvimento têm poucos recursos para contestar determinadas regras impostas pelos países do norte global. Conforme veremos esta controvérsia retornará de forma mais enfática no próximo ano com o debate sobre direitos autorais e pirataria.

Por fim, observa-se que, em 2015, se consolida o debate sobre a Internet das coisas e a coleta de dados no mundo físico. Essa discussão é de extrema relevância, pois representa a dimensão coletiva da privacidade, a importância de que seja debatida para além do ponto de vista liberal de direitos individuais. Neste contexto, há a discussão sobre a propriedade dos dados coletados, como por exemplo nas "cidades inteligentes", em que informações agregadas servem para otimizar os fluxos e sistemas públicos. Estas informações pertencem a quem? Aos cidadãos que as geraram? Ao Estado ou às corporações que a gerenciam? O caráter coletivo da privacidade é o que torna a discussão relevante em termos do exercício da cidadania e direitos democráticos. Realizados estes destaques sobre o debate de 2015 prossegue-se ao ano seguinte.

Em 2016, o Fórum aconteceu entre os dias 6 e 9 de dezembro em Jalisco, no México. Das quatorze sessões principais nenhuma delas abordou diretamente nem o tema da privacidade, nem a

[93] U.S. House to vote to reinstate net neutrality rules in April. https://www.reuters.com/article/us-usa-Internet/u-s-house-to-vote-to-reinstate-net-neutrality-rules-in-april-idUSKCN1R2268. Acessado em 12/8/19.

segurança. Dentre estas atividades a que a palavra "privacidade" obteve mais ocorrências foi a intitulada "Direitos Humanos ampliando a conversa" com trinta e seis (36) entradas. Na ocasião, o termo "vigilância" foi mobilizado em dezessete (17) vezes, "segurança" em apenas nove (9). O termo "direitos" foi mobilizado trezentas e cinco vezes (305) e "liberdade" cinquenta e uma vezes (51).

A plenária "Direitos Humanos ampliando a conversa" foi bastante diversa. Pelo vídeo disponibilizado online observa-se a presença de vinte pessoas no palco[94]. O formato da atividade é de breves exposições dos panelistas e intervenção do público. A seguir destaca-se as principais falas que tratam do objeto de pesquisa, ou seja, a privacidade e sua relação com a democracia.

A primeira intervenção relevante é realizada por Ana Neves, do governo de Portugal. Ela destaca que a Internet modificou hábitos, comportamentos, regras, trabalhos e diversos aspectos da vida das pessoas e que devido a estas transformações na sociedade existe a necessidade de implementar novos padrões de privacidade. Menciona a diretiva de proteção de dados da União Europeia, que se tornaria o Regulamento Geral de Proteção de Dados, com um instrumento de prevenção de abusos e proteção de dados pessoais. Neste contexto, Patrick Penninckx, representante do Conselho da Europa, enfatiza que os direitos sociais são baseados em relações industriais do século 19, muito antes da era digital. Portanto, para ele os Estados enfrentam dificuldades em implementar novos direitos digitais.

Outra intervenção relevante é de Luis Fernando Garcia, do terceiro setor do México, que havia participado da sessão do ano anterior. Ele diz que, apesar da retórica de direitos humanos ter ganhado espaço nos debates sobre governança da Internet, sua implementação é bem diferente na realidade. Afirma que autoridades estatais vigiam seus cidadãos, inclusive em casos em que não há previsão legal. No México, por exemplo, há registros de autoridades sem jurisdição vigiando a população, registros de grampos telefônicos, coleta de dados de usuários sem um mandado judicial, compartilhamento de informações telefônicas, dentre outras violações. Enfatiza que o México é um dos maiores compradores de sofisticados *malwares* de vigilância e que as autoridades que adquirem estas tecnologias sequer possuem jurisdição para vigiar a população.

Por sua vez, Paz Pena, da ONG brasileira *Coding Rights*, enfatiza que a discriminação e o discurso de ódio não apenas aumentaram na opinião pública, mas também influenciaram resultados políticos e eleitorais em várias regiões do mundo. Afirma que não há dúvidas que a Internet é uma ferramenta poderosa para a organização política e participação para aqueles que tem o privilégio de ter acesso à rede. Para ela, este é um momento crítico, pois se observa uma sociedade de dados em que a participação política está mudando para o discurso de ódio, xenofobia etc. Para ela, estamos em

[94] Direitos Humanos ampliando a conversa. Disponível em https://www.youtube.com/watch?v=q3otc-__RDw. Acessado em 12/8/19.

um momento chave em que a Internet se tornará um facilitador do exercício dos direitos humanos, ou será uma ferramenta para controlar os sujeitos por meio da documentação e categorização, criminalização de ativismo, ocupação, gênero, saúde, condições sociais, classe e raça. Trata-se de uma vigilância por parte do Estado, mas também de controle social. Prossegue dizendo que, de uma perspectiva intersecional e de gênero, não é suficiente demandar mais transparência e *accountability* sobre quem possui nossos dados e o que fazem com eles, já que isso apenas irá legitimar uma sociedade de controle. Para ela, é necessário recuperar uma visão democrática de sociedade que está deixando decisões éticas para algoritmos de dados manipulados por terceiros. Finaliza afirmando que é preciso lutar contra o modelo da Internet enquanto uma ferramenta de controle. Propõe o e uso de alternativas às ferramentas atuais como Google e Facebook como uma forma de resistência. Para ela, o software livre pode ser esta instância que garante que as pessoas controlem os próprios dados, suas próprias vidas.

Por sua vez, Rebecca McKinnon, da ONG *Ranking Digital Rights*, contextualiza dizendo que antes da Internet vivíamos em um deserto de dados, que os governos tinham seus sistemas da informação baseados na escassez. Portanto, os sistemas de governança, mecanismos que preveniam o abuso de poder, não são adequados para esse novo ecossistema transfronteiriço. Destaca a importância de ser possível baixar os próprios dados para ver o que as empresas coletaram, bem como a opção de solicitar a exclusão destas informações e de se ter controle sobre as circunstâncias em que a informação pessoal é utilizada.

Novamente, Garcia, do México, destaca que existe uma diferença em se ter vigilância em países que possuem freios e contrapesos institucionais e aqueles que apenas importam princípios e leis do norte global para suas legislações locais. Prossegue dizendo que se deve considerar o colonialismo legal e cita o exemplo da legislação de direitos autorais, que exerce censura em alguns países devido às leis de outros. Enfatiza que é um problema quando autoridades europeias demandam que determinados conteúdos sejam removidos globalmente.

Um comentário relevante da plateia é feito por Stuart Hamilton, que fala sobre a manipulação da informação realizada pelos algoritmos. Em resposta, o representante do Google, comenta sobre os dados que as empresas utilizam para oferecer resultados personalizados. Para ele, uma das grandes forças da Internet é o fato de que se pode obter mais informações de diferentes pontos de vista. Diz que no Google descobriram que a fonte de informação é o melhor indicador do que as pessoas querem.

Por sua vez, Anita Gurumurthy da ONG *IT For Change*, destaca que se deve considerar o fato de que não são apenas dados individuais, porque reduzir o fenômeno dos dados a uma questão de conteúdo pessoal seria incorreto. Para ela, o fenômeno é social, ainda mais quando se pensa no elo entre Estados e corporações. Finaliza destacando que se permitirmos que a questão dos dados se torne uma questão individual estaremos perdendo toda a ideia da democracia social, de quem somos

enquanto comunidade. Neste contexto, o representante do governo cubano diz que a Internet precisa ser vista como parte de um conjunto de tecnologias necessárias para a prestação de serviços básicos, como água potável, eletricidade, alimentação, habitação, educação e saúde.

Outra intervenção relevante é feita por Sally Burch, da *JustNet Coalition* do Equador. Ela destaca que as plataformas da Internet são governadas por algoritmos não transparentes, que assumem o papel de intermediários no compartilhamento de conteúdo, dentre outras funções, que se sobrepõem às regras que as sociedades construíram durante décadas para regular as áreas de interesse público.

A professora Mackinnon ressalta que o foco em remover o discurso de ódio, que basicamente coloca o ônus de nas empresas como a fonte do problema, é falho ao tratar de um problema que tem origem offline. Enfatiza que nos países em que o extremismo é uma grande preocupação, jornalistas independentes e ativistas da sociedade civil estão sendo presos e silenciados. Justamente as pessoas mais propensas a oferecer discursos alternativos ao extremismo.

Ao final, Frank La Rue resume a plenária. Destaca que o direito à privacidade é uma prerrogativa do exercício da liberdade de expressão. Justamente por isso as políticas de vigilância, sejam elas justificadas para combater o crime organizado, o terrorismo, a segurança nacional, todas estas práticas de vigilância, devem ser realizadas dentro do Estado de direito e de forma democrática, sendo transparentes e responsáveis para com a população. Afirma que, se deixarmos que a tecnologia se sobreponha aos direitos, prejudicaremos o futuro das sociedades, tornando-as mais fracas, inclusive em sua segurança nacional, já que a população precisa confiar nas autoridades e no modelo democrático de participação. Finaliza reconhecendo que há uma crise no jornalismo em face às notícias falsas. Encerra admitindo que a Internet está permitindo a concentração de mídia de forma massiva, o que viola os princípios de diversidade e pluralismo das comunicações. Após quase três horas de plenária a atividade é encerrada.

Dentre as controvérsias identificadas no ano de 2016, o colonialismo digital se consolida como uma questão, possivelmente relacionado ao local onde ocorre o Fórum, o México. O abuso de autoridade por parte de integrantes do Estado, sejam eles integrantes do aparato policial e judiciário, mas também do poder executivo, é prática comum, enfatiza Luis Garcia. Ele ainda ressalta que países do sul global estão importando legislações do norte, como se elas fossem se adaptar à diferentes contextos, em práticas que denomina como colonialismo legal. Como exemplo, cita a legislação de direitos autorais da União Europeia, que pode significar censura em alguns países.

De certa forma, ele antecipa o debate sobre uma polêmica diretiva do bloco, que responsabiliza as plataformas sobre o conteúdo publicado por terceiros, controvérsia antiga nos debates sobre governança da Internet, que envolve também o discurso de ódio e a liberdade de

expressão. A diretriz da União europeia sobre serviços de mídia e audiovisual[95], aprovada em 2019, inicialmente, se aplicaria apenas a serviços de rádio fusão (*broadcast*) e provedores de mídia com responsabilidades editoriais, ou seja, aqueles com controle sobre a seleção e organização do conteúdo veiculado. Entretanto, a diretriz acabou por incluir serviços de compartilhamento de vídeos, mercado que o Youtube tem amplo domínio. Ocorre que o controle editorial destas plataformas é diferente daquele realizado pela mídia tradicional, como discutido no primeiro capítulo. A começar pelo fato de que o conteúdo é compartilhado, ou mesmo produzido, pelos próprios usuários, não por corporações de mídia. O enquadramento, agendamento e os processos de gatekeeping também se modificam. O controle editorial é realizado em parte por meio de algoritmos que operam o sistema de recomendações destas plataformas de conteúdo. A norma está prevista para entrar em vigor em setembro de 2020 e, caso seja aprovada neste formato, obrigará as plataformas de mídia a criarem "tecnologias de reconhecimento de conteúdos", que, na prática, são filtros automatizados, que tendem a impor censura a determinado conteúdo.

Trata-se de uma regra regional com impacto global. É neste contexto que finalmente é introduzida outra controvérsia central relativa à forma com que os algoritmos operam nas redes e plataformas. As críticas sobre a falta de transparências destes mecanismos são direcionadas não apenas aos filtros de conteúdo, que, por sua vez, geram as bolhas, ou as câmaras de eco, mas também na manipulação de resultados de buscas, na publicidade online, e na construção de jardins murados, mas também nas decisões automatizadas de sistemas de inteligência artificial, ou aprendizado de máquinas. Estes algoritmos categorizam e discriminam pessoas, tomando decisões que impactam a sociedade, por isso a proteção de dados pessoais não pode ser resumida a uma questão individual, já que seu caráter coletivo está cada vez mais evidente, especialmente a partir da expansão da Internet das coisas. A controvérsia sobre a forma de funcionamento dos algoritmos é central no debate sobre privacidade e proteção de dados pessoais.

Importante destacar ainda que os temas das notícias falsas, do extremismo e do discurso online são abordados a partir da perspectiva eleitoral, justamente no ano em que posteriormente se revelaria como central para escândalos de manipulação do eleitorado como o *Cambridge Analytica* e as eleições presidenciais estadunidenses. O debate realizado no México em 2016 antecipa essa discussão com ênfase nos processos dos países do sul global, em que o respeito aos direitos humanos ainda são um desafio, assim como os controles institucionais entres os três poderes.

Portanto, a controvérsia sobre liberdade de expressão, moderação de conteúdo, discurso de ódio se consolida como um dos principais debates que envolvem a privacidade, a proteção de dados

[95] Parlamento Europeu aprova diretiva sobre os direitos de autor. Disponível em < http://www.europarl.europa.eu/news/pt/press-room/20190321IPR32110/parlamento-europeu-aprova-diretiva-sobre-os-direitos-de-autor>. Acessado em 12/8/19.

e o exercício da cidadania na contemporaneidade. É justamente neste contexto que a privacidade se destaca como um direito para o livre exercício da liberdade de expressão, pois as pessoas tendem a praticar a auto censura quando têm conhecimento das práticas de vigilância dos governos e empresas, especialmente em países em que o abuso de poder é prática de Estado.

Inclusive, dentre as mil seiscentos e cinquenta (1650) vezes que o termo "liberdade" é mobilizado nos discursos nas sessões principais do Fórum, mais da metade – oitocentos e quinze (815) vezes – ele é acompanhado pela palavra "expressão". Portanto, seus interlocutores referiam-se a um tipo específico de liberdade, não apenas a liberdade como um conceito amplo relacionado às liberdades individuais do liberalismo. A palavra "liberdade" varia da seguinte forma ao longo dos anos;

Gráfico 6: Mobilização da palavra "liberdade" nas sessões principais do Fórum.

Fonte: Autora a partir de dados extraídos do site.

A palavra "liberdade" foi mais mobilizada em 2013, justamente o único ano em que a liberdade de expressão foi título das sessões principais do Fórum. Na ocasião o termo foi mobilizado em duzentas e seis (206) vezes. Por sua vez, o ano em que obteve menor recorrência foi o de 2008, justamente o Fórum em que a palavra "segurança" obteve seu maior índice. A queda no ano de 2014 acompanha todos os outros termos. Por outro lado, a palavra é menos mobilizada nos anos recentes, ainda que o exercício da liberdade de expressão ganhe centralidade no debate sobre privacidade e

proteção de dados pessoais, principalmente devido ao controle privado da veiculação de conteúdo online e os algoritmos de recomendação da web. Com a consolidação das plataformas de conteúdo como *gatekeepers* da rede, o debate sobre os critérios de priorização, ou remoção de conteúdo ganham centralidade. Sua influência em processos eleitorais e a propaganda política na web retoma questões sobre a transparência das decisões dos algoritmos e o controle dos usuários sobre as próprias informações.

É neste contexto que se consolida a controvérsia sobre a concentração de poder das grandes plataformas de conteúdo da web, que além de violar práticas concorrenciais, determinam regras comerciais para a veiculação de conteúdo. A propaganda política, discursos misóginos, racistas e xenófobos são permitidos devido aos interesses comerciais das plataformas, que não levam em consideração princípios democráticos de diversidade e pluralismo das comunicações ao determinar as regras sobre os conteúdos veiculados. De fato, elas tornam equivalentes todo o tipo de argumentação, independente se o conteúdo é jornalístico, ou seja, verificado, ou simples desinformação.

Inclusive, neste ano de 2016, o Facebook estabeleceu novas regras para ordenar a forma com que as pessoas interagem com as informações, privilegiando "amigos e familiares" em detrimento de links de outros websites[96]. Na prática, isso forçou as empresas de jornalismo a anunciarem na plataforma, ou simplesmente seriam ignoradas pelos algoritmos que determinam o que as pessoas veem por lá. Ainda assim, há de se ponderar que a web faz parte de um ecossistema de mídia marcado por assimetrias e concentração de poder, portanto, de certa forma, a Internet está reproduzindo um padrão histórico do setor de telecomunicações.

Realizadas estas considerações prossegue-se à análise da edição de 2017 do Fórum, que aconteceu entre 18 e 21 dezembro, em Genebra, na Suíça. Na ocasião, ocorreram doze sessões principais. Dentre elas, a atividade em que o termo "privacidade" teve mais ocorrências – sendo mobilizada vinte e duas (22) vezes - foi a intitulada "Intervenções Locais, Impactos Globais: Como a Cooperação Internacional Multissetorial pode tratar das rupturas da Internet, da Criptografia e do Fluxos de Dados". Durante a atividade a palavra "segurança" foi utilizada em cinquenta e nove (59) vezes, "vigilância" nove (9) vezes, "direitos" quarenta e uma (41) vezes, "liberdade" treze vezes (13).

Antes de avançar é importante pontuar que a segurança volta a estar presente nas plenárias com a atividade "Fortalecendo a cooperação global em cibersegurança para o desenvolvimento sustentável e a paz". Na ocasião a palavra "segurança" foi mencionada duzentas e seis vezes (206), a "privacidade" apenas cinco vezes (5), "vigilância" apenas duas (2), direitos vinte e três (23) e

[96] Facebook to Change News Feed to Focus on Friends and Family. Disponível em https://www.nytimes.com/2016/06/30/technology/facebook-to-change-news-feed-to-focus-on-friends-and-family.html. Acesso em 23/12/19.

"liberdade" (6) apenas seis. Estes dados quantitativos indicam que o tema da segurança foi discutido muito mais da perspectiva técnica e de cooperação internacional do que uma abordagem de direitos humanos, privacidade e proteção de dados pessoais.

A plenária em que o termo "privacidade" foi mais mobilizado, foi dividida em três segmentos correspondentes a seu título; cooperação internacional, criptografia e fluxos de dados. À medida em que o debate ocorria, os palestrantes se retiravam do palco para dar espaço a outros debatedores, em um formato diferente dos anos anteriores, conforme observa-se no registo em vídeo da atividade[97].

Na primeira etapa da plenária, o tema da privacidade foi muito pouco mobilizado. Dentre os palestrantes, o único a mencionar a questão foi Demi Getschko, do CGI.br, ao citar que o Marco Civil da Internet está estruturado em três pilares; a privacidade, a neutralidade da rede e a liberdade de expressão. Já a segunda parte da atividade, sobre criptografia, o tema foi mais recorrente.

Dentre os palestrantes, destaca-se a intervenção de Riana Pfefferkorn, da Universidade de Stanford, nos Estados Unidos, que enfatiza que é vital para as democracias do mundo respeitar e apoiar o uso da criptografia, tanto para a comunicação, quanto para o armazenamento de dados. Por sua vez, Raúl Echeberría, da Internet Society do México, enfatiza como a criptografia é importante para a proteção de dados pessoais, citando, por exemplo, o sigilo das transações financeiras.

Já Moctar Yedaly, da *African Union Commission*, destaca que a África é uma das poucas regiões do mundo que adotou uma convenção sobre proteção de dados pessoais ainda em 2010, antecipando-se em interconectar a proteção de dados e a cibersegurança. Explica que a convenção regional possui três grandes eixos; transações eletrônicas, proteção de dados pessoais e promoção da cibersegurança. Para ele, um dos grandes avanços é que a convenção define o que é criptografia, especifica as ferramentas e os meios disponíveis para utilizá-la.

Por sua vez, Luis Fernando García, da ONG mexicana R3D, destaca a importância da criptografia para proteger a segurança, a privacidade, a liberdade de expressão e o anonimato. Novamente cita o exemplo de seu país, em que há regiões em que a violência é tão grave que a mídia tradicional não se atreve a fazer reportagens sobre o que ocorre. Nestas chamadas "zonas de silêncio" a mídia digital e os jornalistas independentes são as únicas fontes de informação e, para eles a criptografia e privacidade são ferramentas essenciais para proteger suas vidas e a de suas fontes. Já Paul Nichols, da Microsoft, destaca que a criptografia é fundamental para o gerenciamento de riscos nos negócios modernos, pois é como se protegem as operações.

Na terceira parte da plenária, sobre fluxos de dados, o tema da privacidade é pouco mobilizado. Dentre as falas dos palestrantes, destaca-se a de André Laperriére, do *Global Open Data*

[97] Intervenções Locais, Impactos Globais: Como a Cooperação Internacional Multissetorial pode tratar das rupturas da Internet, da Criptografia e do Fluxos de Dados. Disponível em https://youtu.be/9ZvsHZsJSlE. Acessado em 12/8/19.

Initiative for Agriculture and Nutrition, que enfatiza a anonimização como um importante recurso para garantir a privacidade e que as pessoas devem poder escolher com quem compartilham suas informações, ou seja, tenham o controle sobre os dados pessoais.

Por fim, Anne Carblanc, da Organização para a Cooperação e Desenvolvimento Econômico (OECD), destaca que as diretrizes sobre criptografia da organização existem há vinte anos e são revisadas com frequência. Explica que o documento reconhece que as políticas de criptografia nacionais podem permitir o acesso legal aos dados, às chaves de criptografia, ou a dados criptografados. As diretrizes destacam a questão da responsabilidade, atestando que aqueles que tiverem acesso aos dados criptografados podem ser responsabilizados em casos de quebra de segurança. Por fim, o documento enfatiza o respeito à privacidade e o direito à escolha dos métodos de criptografia. Outras intervenções são realizadas sem tratar do tema da privacidade até que a plenária é encerrada.

Em termos da análise qualitativa, inicialmente, é importante enfatizar que pela primeira vez o tema da criptografia ganha destaque em uma sessão principal do Fórum. Por outro lado, a plenária de 2017, até por não tratar diretamente do tema da privacidade, não apresenta novas controvérsias. Ainda assim, há alguns pontos importantes. Dentre eles, ressalta-se a anonimização de dados enquanto um recurso adicional à privacidade. Esta técnica, somada à criptografia fortalece os mecanismos de proteção de dados. Neste sentido, vale destacar que, tanto o representante do setor privado, como a da OCDE, destacam a criptografia enquanto uma ferramenta importante para o próprio mercado, o que contribui para que esta técnica seja mais difundida.

Em 2018, o Fórum ocorre entre 12 e 14 de novembro em Paris, na França, com treze sessões principais. Neste ano, o tema da privacidade retorna às atividades principais com a plenária "Cibersegurança, confiança e privacidade[98]". Na ocasião o termo "privacidade" foi mobilizado apenas dezesseis (16) vezes, "segurança" 73 vezes, "direitos" 21 vezes, "liberdade" apenas 10 vezes. A palavra "vigilância" não obteve nenhuma ocorrência. Trata-se da atividade principal que possui a palavra privacidade em seu título, mas que obtém o menor número de ocorrências dentre as falas dos participantes. O formato da atividade foi o de painel, com os palestrantes ao palco.

Dentre as falas iniciais dos palestrantes é importante ressaltar que os representantes governamentais - Long Zhou da China e David Martinon da França – focaram essencialmente na questão de segurança. O mesmo pode ser dito sobre a fala de Christoph Steck da empresa Telefônica. O contraponto é realizado por Mallory Knodel, da ONG internacional Artigo 19, que critica o foco excessivo na questão da cibersegurança afirmando que o foco deste tipo de debate deve ser as pessoas,

[98] Cibersegurança, confiança e privacidade. Disponível em < https://www.intgovforum.org/multilingual/content/igf-2018-day-2-salle-i-cybersecurity-trust-privacy>. Acesso em 23/12/19.

não as economias ou os negócios. Adiante no debate a questão da privacidade é abordada por outra representante do terceiro setor, Ashnah Kalemera, da ONG africana CIPESA. Ela pondera que boa parte das legislações sobre cibersegurança debilitam o direito à privacidade. Os dados quantitativos que apontam o baixo índice da mobilização do termo privacidade refletem também na análise qualitativa, que não identificou novas controvérsias no debate, apenas a evolução de algumas já verificadas em anos anteriores. Dentre elas, o balanço entre a proteção de dados pessoais em legislações sobre cibersegurança.

Já em 2019, o Fórum ocorreu de 25 a 29 de novembro em Berlim, na Alemanha e contou com onze sessões principais, dentre as quais nenhuma abordou diretamente a privacidade, apenas a questão da cibersegurança. Dentre elas, a que o termo "privacidade" obteve maior recorrência – com dezoito entradas - foi a trilha "Tecnologias emergentes e suas interfaces com a inclusão, a segurança e os direitos humanos[99]". Na ocasião a palavra "segurança" obteve quarenta e cinco (45) ocorrências, "direitos" vinte e duas (22), "vigilância" duas e "liberdade" apenas uma.

O formato da atividade se modifica. As moderadoras ficam no palco e há uma mesa redonda com cerca de trinta cadeiras, além da plateia. A sessão funcionou como uma plenária em que representantes de Fóruns da Internet locais reportaram sobre o que debatiam com relação ao tema das tecnologias emergentes em suas regiões. Poucos participantes expressaram receios com relação a proteção de dados pessoais diante da expansão da internet das coisas, da inteligência artificial, o uso de drones, realidade aumentada, dentre outras tecnologias como o blockchain (este último realmente capaz de ampliar a privacidade online, devido a seu sistema de criptografia).

Alguns participantes apenas citaram a questão da privacidade, sem aprofundar a questão. Uma das exceções foi o brasileiro José Luiz Ribeiro Filho que disse que a questão do reconhecimento facial é muto discutida no país devido seu uso por parte das autoridades policiais. Ele demonstrou receio de que estes sistemas impactem interações sociais em termos de diversidade e respeito a minorias. Afirmou ainda que muitas organizações no país questionam tecnologias cujo objetivo principal é categorizar indivíduos de forma automatizada por meio de sistemas de inteligência artificial.

Por sua vez, Nancy Carter, do Canadá, contou que estima-se que haja 114 milhões de dispositivos da internet das coisas em funcionamento no país. Criticou o fato deles não adotarem a privacidade por padrão, questão que é debatida pela autoridade local de proteção de dados. Já, Eun Chang Choi, da Coréia do Sul, disse que o governo local está investindo em tecnologias que tornam os dados anonimizados para ampliar seu uso público. Há uma lei local que determina a

[99] Emerging technologies and their interfaces with inclusion, security and human rights. Disponível em < https://www.intgovforum.org/multilingual/content/igf-2019-%E2%80%93-day-3-%E2%80%93-convention-hall-ii-%E2%80%93-emerging-technologies-and-their-interfaces-with >. Acesso em 2/2/20.

"desentificação" de dados pessoais. Em paralelo, o governo local está buscando atualizar sua legislação para os padrões do regulamento europeu de proteção de dados.

Outra participante que mobilizou o tema da privacidade foi a representante do Panamá (cujo nome não foi identificado na transcrição tampouco no vídeo). Ela contou que o Fórum local teve como tema principal a privacidade e proteção de dados pessoais. Disse ainda que devido a localização do país – entre México e Colômbia – existem muitas preocupações sobre segurança e que o governo local busca resolver estes desafios ampliando a vigilância com tecnologias invasivas. Contou que há um aumento expressivo do uso de biometria no país o que coloca em risco a privacidade dos cidadãos.

Já Jennifer Chung, do Fórum regional da Ásia, citou a resolução 68/167 das Nações Unidas sobre o direito à privacidade na era digital que atesta que a vigilância arbitrária contradiz os princípios de uma sociedade democrática[100]. Disse ainda que o Fórum local debateu muito sobre as classificações realizadas por algoritmos inteligentes, que reproduzem preconceito a partir de interpretações subjetivas.

Sendo assim, a análise qualitativa do debate indica que a questão da privacidade foi abordada associada à expansão da Internet das coisas e da inteligência artificial. Estas controvérsias já haviam sido identificadas nos anos anteriores e foram apenas aprofundadas em 2019. Ainda assim, é importante ressaltar que o debate sobre a ética envolvida na tomada de decisões dos algoritmos inteligentes se intensifica. Trata-se de uma questão central que se complementa à regulação de dados pessoais. Além disso, a expansão de tecnologias como o reconhecimento facial e a identificação biométrica ampliam a preocupação com relação à privacidade.

[100] Resolution adopted by the General Assembly on 18 December 2013 -68/167. The right to privacy in the digital age Disponível em https://undocs.org/A/RES/68/167. Acesso em 2/2/20.

4 – Considerações finais

O conceito de privacidade, estruturado a partir da distinção entre público e privado, remete à uma metáfora espacial que perde sentido com a introdução das tecnologias da informação. A proteção de dados pessoais ganha relevância a partir do momento em que os algoritmos permeiam os mais diversos aspectos da vida em sociedade. A dimensão coletiva destas questões as tornam objeto de reflexão no contexto das teorias da democracia contemporâneas.

A relação entre estes temas – algoritmos, privacidade e democracia – foi explorada a partir da revisão de literatura e uma análise empírica de discursos no âmbito do Fórum de Governança da Internet. Estas reflexões indicam alguns resultados. Em primeiro lugar, destaca-se a importância de abordar os temas da privacidade e da proteção de dados pessoais a partir de uma perspectiva coletiva, não apenas como um direito individual. O capitalismo – ou neoliberalismo – de vigilância desafia as democracias liberais não apenas por influenciar em seus processos políticos e eleitorais, mas principalmente por tornar as experiências privadas como fonte de lucro e vantagem mercadológica de grandes empresas de tecnologia.

A esfera privada, historicamente negligenciada na teoria política, torna-se a principal origem de informação do mercado de dados. Neste contexto, é desafiador pensar que a privacidade, defendida enquanto um direito humano fundamental, seja cotidianamente deixada de lado por metade da população mundial, que utiliza as tecnologias da informação e comunicação. Este paradoxo é justamente o que a torna objeto de uma questão coletiva. As pessoas são levadas a ignorar a questão da privacidade e da proteção de seus dados pessoais de acordo com situações sociais complexas, já que cada vez mais as tecnologias fazem parte dos mais diversos aspectos da vida social.

O tratamento de dados pessoais incide cada vez mais no exercício da cidadania, dos direitos e das liberdades individuais. As normas jurídicas e instituições não podem mais negligenciar o que ocorre na esfera privada, que se torna cada vez mais política. A interação e a própria participação política se deslocam da esfera pública para a privada, por intermédio das tecnologias da informação e comunicação. Estas transformações tornam evidente o fato de que a privacidade não é apenas o direito de ser deixado em paz, mas também condição para o desenvolvimento da própria personalidade dos sujeitos contemporâneos. A privacidade é estruturante da própria democracia liberal, em que o voto secreto constitui a expressão da autorização da representação.

Em segundo lugar, paradoxalmente, observa-se a perda da centralidade do debate sobre o direito à privacidade. O fato de que há um constante monitoramento das experiências privadas pelos sistemas cibernéticos parece não ser um problema. Por vezes, essa intermediação é até útil no cotidiano das pessoas. Aparentemente há uma resignação coletiva, como se o fim da privacidade fosse realmente inevitável. Nem a própria irrelevância nos livra do fato de que nossos dados alimentam o

capitalismo de vigilância.

Os dados resultantes da análise empírica ilustram este fenômeno; o escândalo de 2013 das revelações de Snowden é seguido por um silenciamento sobre o tema, não apenas no âmbito do Fórum. Com a ascensão da computação móvel o próprio software livre perde relevância nos debates sobre tecnologia e sociedade. Se, por um lado, a discussão sobre privacidade perde centralidade, a questão da proteção de dados pessoais ganha destaque com a entrada em vigor de legislações que tratam do tema.

Se consolida, no âmbito da União Europeia, o principal marco normativo sobre privacidade e proteção de dados pessoais contemporâneo. O Regulamento Geral sobre Proteção de Dados reflete uma visão de democracia em que o Estado é protetor dos direitos e liberdades individuais, que reflete o estado de bem estar social do período pós guerra. A legislação busca conter o avanço das empresas de tecnologia e seu modelo de negócios estruturado no mercado de dados a partir de mecanismos de consentimento informado e limitação das finalidades de coleta de informações. Somado à isso há o fato de que a União Europeia, que não deixa de ser neoliberal, ocupa uma posição estratégica na geopolítica mundial, portanto tem força para conter o avanço das empresas de tecnologia, em sua maioria localizadas nos Estados Unidos.

Ainda assim, é preciso enfatizar que não se trata de uma intervenção arbitrária, pelo contrário. A legislação é resultado de debates realizados ao longo de mais de trinta anos. A regra, após aprovada em 2016, levou ainda dois anos para entrar em vigor. As empresas possuem outros dois anos para se adaptarem à regulação, ou seja, até maio de 2020.

O Regulamento Geral sobre Proteção de Dados é a legislação que mais garante os direitos dos cidadãos em controlar as próprias informações, sendo responsável ainda por estabelecer novas regras para o setor de tecnologia. O regulamento inspirou outros marcos normativos ao redor do mundo; a lei geral de proteção de dados brasileira, prevista para vigorar a partir de agosto de 2020, e a Lei de Privacidade do Consumidor da Califórnia, válida desde janeiro de 2020. Esta confluência da vigência de normas sobre proteção de dados pessoais torna a virada de década um ponto chave no debate.

Por outro lado, em termos práticos, para a população em geral, as mudanças foram muito discretas. As alterações de configuração dos websites incorporaram avisos legais (*disclaimers*) sobre o uso de cookies e dos dados pessoais para melhorar a experiência de uso. As notificações sobre os termos de uso e a política de privacidade ganharam destaque nas páginas web em mensagens que surgem logo no primeiro acesso. Entretanto, há aí uma ironia. Em sua vasta maioria estes avisos apresentam apenas a opção de "aceitar" para que o site ou aplicativo seja acessado. A margem de negociação continua sendo mínima. Ou você aceita os termos impostos, ou não ingressa no serviço ou informação desejada. As opções de saída – *opt-out* – são extremamente limitadas. Neste sentido, pode-se concluir que o design das plataformas e dispositivos da internet das coisas mudou muito

pouco, sendo ineficiente em incorporar a privacidade por padrão.

É neste contexto que se avalia que os marcos normativos sobre proteção de dados pessoais se mostraram insuficientes para conter o avanço do mercado de dados e a concentração de poder das empresas de tecnologia. De forma semelhante, as leis estadunidenses de antitruste tampouco preveniram que as gigantes da FAMGA ampliassem seu monopólio no setor de tecnologia. O próprio mercado financeiro se fundiu com estas companhias, dado que são controladas pelos mesmos agentes. A expansão do neoliberalismo aprofundou as desigualdades em níveis mundiais; ricos cada vez mais ricos e pobres cada vez mais pobres.

Se o cenário do norte global indica alguma perspectiva de mudança, com o fim do prazo de tolerância do regulamento europeu e a nova lei californiana, o panorama para o sul global é bem distinto. Países com sistemas democráticos frágeis e governos autoritários tornam-se alvo de experimentos tecnológicos de vigilância, que vão do cadastro biométrico, passam pelo reconhecimento facial, o uso de drones e até mesmo a criação de bancos de dados de DNA. Em locais em que o sistema de justiça e os contrapesos institucionais são fracos, não basta uma lei geral de proteção de dados, até porque os próprios direitos humanos são pouco respeitados. Observa-se assim a expansão do mercado de tecnologia por meio do colonialismo digital e legal.

Regular o setor de tecnologia é um desafio, dado que o trâmite legislativo, na maioria das vezes, não acompanha a rapidez e evolução deste setor. Ainda assim, é dever do Estado intervir para garantir o exercício dos direitos e das liberdades individuais. Para os liberais, pode-se argumentar que se trata de assegurar as bases do livre mercado, ou seja, um ambiente comercial justo, aberto e competitivo, que beneficie os consumidores. Para setores que se preocupam com os direitos humanos as alegações são ainda mais simples; é papel do Estado garantir que a economia não se sobreponha à política e aos valores democráticos.

Por todos estes fatores a grande controvérsia em torno dos debates sobre privacidade e proteção de dados pessoais identificada na análise empírica das sessões principais do Fórum de Governança da Internet é com relação ao marco regulatório do setor de tecnologia, não apenas as normas sobre proteção de dados. Dada sua natureza transfronteiriça, seus impactos são globais e afetam, cada vez mais, toda a população mundial, ainda que, conforme discutido, cidadãos do norte global estejam mais assegurados por suas instituições. Se a União Europeia tem uma abordagem mais social democrata quando se trata de regular o setor, o modelo estadunidense, em sua maioria, funciona após casos concretos, sendo ineficiente em termos de prevenção. Ou seja, as leis são criadas depois que o dano já foi feito. Trata-se do modelo neoliberal de auto regulação, em que a intervenção do Estado é vista como negativa. Além disso, é uma perspectiva que enxerga o exercício da cidadania a partir dos direitos dos consumidores.

O marco regulatório da mídia tradicional não se adapta facilmente à web, seja no modelo de

concessões, na ampliação da infraestrutura, na medição de audiência, na veiculação de propaganda, na proteção da privacidade, ou dos direitos dos consumidores. É neste contexto que se identifica a segunda grande controvérsia envolvendo os debates sobre privacidade no âmbito das edições do Fórum de Governança da Internet; a responsabilização dos intermediários sobre o conteúdo publicado por terceiros.

Esta discussão não tem correspondência na mídia tradicional, justamente porque estes meios possuem controle editorial sobre o que é publicado. Na web cada pessoa divulga o que quiser. A jurisprudência estadunidense, onde estão sediadas as principais companhias de tecnologia, tem como base uma lei de combate à pornografia de 1996, portanto anterior à própria indexação da web. O Marco Civil da Internet brasileiro segue na mesma direção, eximindo os provedores de responsabilidade sobre o conteúdo publicado por terceiros. Já no âmbito da União Europeia a discussão se torna mais complexa, não estruturada em princípios pré determinados. O ponto central deste debate é o exercício da liberdade de expressão e seus limites.

Um dos principais marcos dessa discussão foi a decisão da Autoridade de Proteção de Dados da Espanha, em 2014, que garantiu o direito à desindexação – o que difere do direito ao esquecimento. Dois anos depois, o Regulamento Geral sobre Proteção de Dados consolidou o direito à solicitação de apagamento dos próprios dados, que consiste na remoção de conteúdo com base em critérios tais como fatos irrelevantes, ocorridos há muito tempo, ou considerados inadequados. Desde que a regra entrou em vigor, os países do bloco passaram a adotar a política de notificação e retirada (*notice and take down*). Isto faz com que os provedores removam conteúdo da Internet a partir de uma notificação. O ponto central é quem faz esta determinação.

No Brasil a retirada de conteúdo da web ocorre apenas mediante determinação judicial. Nos Estados Unidos, além da determinação judicial, os provedores podem remover material que infrinja os direitos autorais, ou que sejam ilegais. Entretanto, a fronteira entre o que é ou não ilícito é diferente culturalmente e varia entre os países. Certamente há algum consenso sobre os "quatro cavaleiros do info apocalipse" (Assange, 2013), ou seja, lavagem de dinheiro, drogas, terrorismo e pornografia infantil, que justificam a retirada de conteúdo.

Ocorre que estas limitações não foram suficientes para a propagação de discurso de ódio e da desinformação na web. Nestes casos, inicialmente, deixou-se à cargo do setor privado distinguir sobre o que era ou não retirado do ar. Desta forma, as plataformas de conteúdo tornaram-se os gatekeepers da informação que circula na web, em especial nas mídias sociais. Suas regras pouco transparentes indicam que foram criados filtros para revisão prévia e automatizada de conteúdo. Com isto, ao tentar combater estes fenômenos, acabaram por instituir mecanismos de censura e limitação da liberdade de expressão, afetando a opinião pública enquanto um todo.

No caso do discurso de ódio, em 2016, a União Europeia assinou em conjunto com as

plataformas de conteúdo, um código de conduta para combater o avanço da discriminação devido à raça, cor, religião, orientação sexual, descendência, origem nacional ou étnica[101]. No segundo caso, iniciativa semelhante ocorreu em 2018[102]. Entretanto, apenas a legislação alemã – NetzDG - prevê relatórios sobre os processos de decisão envolvidos na curadoria de itens retirados do ar. Este mecanismo garante a transparência das plataformas de conteúdo sobre o que é retirado do ar e por qual motivo.

Longe de esgotar esta controvérsia, que poderia ser tema de uma tese inteira, o que se observa é que a legislação, muitas vezes, foca no aspecto final da questão, ou seja, a remoção de conteúdo na web. Argumenta-se aqui que o arcabouço legal deve transpor-se para a regulação dos processos das empresas de tecnologia; como operam os algoritmos? É possível afirmar que as decisões de inteligência artificial são tomadas em bases éticas e princípios democráticos? De que forma funcionam os mecanismos de recomendação? Quais são os critérios de priorização de conteúdo? Como as máquinas aprenderam a auto completar o resultado das buscas realizadas na web? Elas reproduzem preconceitos? O que é considerado conteúdo inapropriado? Como funcionam os filtros e revisão prévia de conteúdo? Estas são decisões técnicas pelas quais as empresas de tecnologia podem ser responsabilizadas, pois elas são intrínsecas a seu modelo de negócios. São aspectos técnicos que as companhias controlam, muito mais que a publicação de conteúdo ilegal por terceiros.

Esta avaliação sobre a controvérsia da remoção de conteúdo online conduz à segunda conclusão do trabalho; é cada vez mais urgente regular os próprios algoritmos que operam a web, os sistemas de aprendizado de máquinas, o software dos carros autônomos, dos celulares e todos sistemas cibernéticos que fazem a intermediação do cotidiano das pessoas. É necessário dar publicidade aos processos decisórios dos algoritmos inteligentes. A transparência, que está presente no discurso neoliberal de desenvolvimento, torna-se fundamental na regulação do setor de tecnologia. Ainda assim, ela é apenas um primeiro passo. A abertura dos códigos em si não resolve a questão dos algoritmos inteligentes e suas decisões que causam efeitos na sociedade.

Ocorre que estes códigos, na jurisprudência estadunidense, são propriedade intelectual e devem ser mantidos em sigilo para não serem copiados pela concorrência, impactando assim, seu modelo de negócios. Em termos de direito comercial, as patentes destes sistemas deveriam ser públicas de forma a garantir a transparência, mas não é o que ocorre, pois os algoritmos são mantidos em segredo industrial.

As iniciativas *open source* demonstram a viabilidade financeira de operar negócios de

---

[101] European Commission and IT Companies announce Code of Conduct on illegal online hate speech. Disponível em < https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1937>. Acesso em 2/1/20.
[102] Code of Practice on Disinformation. Disponível em < https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>. Acesso em 2/1/20.

tecnologia com códigos abertos. O grande exemplo é o próprio sistema operacional Android – que tem o código aberto, mas um modelo de licenciamento fechado – que domina o mercado de celulares e se expande para relógios, televisores e outros aparelhos digitais.

A questão chave, portanto, não é apenas a abertura dos algoritmos, mas sim seu modelo de licenciamento fechado. A licença de uso do software livre se difere do *open source* justamente por garantir que sistemas derivados devem permanecer abertos. Trata-se de uma aproximação tanto com o ideal de Merton de que toda pesquisa cientifica que produza dados deve ser compartilhada livremente visando o bem comum, como da lógica de Kant sobre a *Publizitat*; o que não é revelado tende a ser injusto.

Sendo assim, o ponto central é a forma de licenciamento dos termos de uso de serviços e aplicativos digitais, que transmite às plataformas ampla liberdade no tratamento de dados pessoais, inclusive sua utilização comercial por "terceiros". É necessário inverter esta lógica para combater a expansão do "neoliberalismo de vigilância". A propriedade dos dados gerados nos sistemas cibernéticos deve ser coletiva, não privada. É neste contexto que se fala em bases de dados públicas – no sentido de pertencimento comum - e criptografadas, em que as pessoas controlam quais informações são disponíveis para quem. A segurança, a autorização e o consentimento devem ser a base dos termos de uso, não a propriedade. Trata-se de uma outra visão de democracia digital, que pode contribuir para uma discussão sobre a ética dos algoritmos. Neste contexto é preciso considerar ainda contratos tecnológicos que violam os direitos humanos e os próprios sistemas democráticos[103].

Por fim, há a controvérsia da dualidade e complementariedade entre privacidade e segurança, principal argumento mobilizado para justificar a vigilância. Inclusive, a análise empírica revelou uma predominância da preocupação sobre a segurança, até mesmo sobre os próprios direitos humanos. A questão da cibersegurança foi a mais mobilizada nos discursos das sessões principais do Fórum de Governança da Internet, superando os direitos humanos. Ocorre que, na teoria clássica do contrato social, as pessoas renunciam à determinadas liberdades em troca da segurança oferecida pelo Estado, o único legítimo a exercer a autoridade de interferir na esfera privada (Hobbes, 1987). Atualmente, o paralelo com os termos de uso das plataformas e aplicativos digitais, reflete como estes acordos são feitos sobre condições impossíveis de não serem aceitas, o que leva as pessoas a abdicarem determinadas liberdades, como a de não ser vigiado. Desta forma o exercício dos direitos deixa de ser indivisível, inter-relacionados e interdependentes, corroendo as bases dos direitos humanos e das democracias liberais contemporâneas. A alienação de direitos realizada por meio dos termos de uso,

[103] Como a tecnologia pode ajudar governos a virarem ditaduras?. Disponível em < https://yaso.blogosfera.uol.com.br/2020/01/18/como-a-tecnologia-pode-ajudar-governos-a-virarem-ditaduras/ >. Acesso em 20/01/20.

torna-se portanto um problema central para a teoria política. É neste contexto que se defende que o Estado precisa intervir para transformar o atual modelo de gestão de bases de dados coletivos.

Realizadas estas considerações finais, conclui-se que os objetivos do trabalho foram alcançados a partir da revisão de literatura e da análise empírica que demonstrou como ocorrem as controvérsias entre sociedade civil, empresas e governos quando o tema é tecnologia e sociedade. Ao longo da tese foi exposto como o tratamento de dados pessoais incide, de diversas formas, no exercício da cidadania, dos direitos e liberdades individuais. Além disso, demonstrou-se como o mercado de dados tornou-se uma preocupação coletiva para as democracias contemporâneas. Enfatizou-se que é necessário aplicar critérios de justiça também na esfera privada.

A partir da análise dos principais marcos regulatórios sobre proteção de dados pessoais conclui-se que o Estado deve regular outras questões intrínsecas ao setor de tecnologia, em especial o modelo de funcionamento dos algoritmos e os termos de uso dos aplicativos e plataformas digitais. A análise empírica dos debates das sessões principais do Fórum de Governança da Internet identificou ainda as seguintes controvérsias; a ineficiência de regulação do setor de tecnologia, a responsabilidade das plataformas sobre o conteúdo veiculado e seus impactos no debate público e sistemas democráticos eleitorais.

A metodologia combinatória de análise, somada à revisão de literatura, contribui para que temas complexos, que causaram uma modificação estrutural sociedade, tanto no âmbito econômico quanto político e social, sejam avaliadas. A pesquisa empírica sobre os marcos regulatórios de proteção e dados pessoais, somada a análise dos discursos mobilizados nas sessões principais do Fórum de Governança da Internet colaboram na compreensão de distintas visões de democracia. Ao enfatizar o aspecto coletivo da privacidade e da proteção de dados pessoais o trabalho busca atentar às teorias da democracia como as tecnologias da informação e comunicação incidem cada vez mais no exercício da cidadania e dos direitos e liberdades.

No início do trabalho enfatizou-se que o sistema representativo e eleitoral tem como base formulações que datam do século XVIII. A teoria política clássica foi estruturada a partir da exclusão das mulheres do espaço público e de um ponto de vista masculino com relação às principais questões das ciências sociais; a noção de indivíduo, de autonomia, de igualdade, de justiça e o próprio conceito de democracia. A invisibilidade da mulher no século XVIII tem um paralelo contemporâneo; o silencioso fenômeno do capitalismo de vigilância, estruturado a partir do tratamento de dados pessoais.

A teoria política feminista colaborou para repensar categorias estruturantes do pensamento social como a distinção entre as esferas público e privada, as relações de poder - dominação e autonomia, igualdade e diferença, diferentes formas de opressão – e até mesmo o que se compreende como identidade. Sobretudo as diversas correntes desta linha de pensamento anteciparam um debate

essencial para os estudos de software; a propriedade dos dados. É neste contexto que este trabalho busca contribuir com reflexões sobre tecnologia e sociedade, democracias digitais, teorias da vigilância e a proteção de dados pessoais já que as informações privadas são cada vez mais uma questão política no século XXI.

Referências

ALLEN, Anita L. **Uneasy access: Privacy for women in a free society**. Londres, Rowman & Littlefield, 1988.

ALMEIDA, Márcia Andréia da Silva et al. **Direitos do consumidor**. São Paulo, IDEC, 2002.

ASSANGE, J. **Cypherpunks**: liberdade e o futuro da Internet. São Paulo: Boitempo. 2013.

BABBIE, Earl R. **The practice of social research**. Nelson Education, 2015.

BAGNOLI, V.Direito da Concorrência: Visão Geral. **Revista Direito Mackenzie**. São Paulo, p. 221 -235, 2002.

BARBROOK, Richard. **Futuros imaginários**: Das máquinas pensantes à aldeia global. São Paulo, Editora Peirópolis LTDA, 2009.

BARZILAI-NAHON, Karine. Gatekeeping: A critical review. **Annual Review of Information Science and Technology**, Chicago, v. 43, n. 1, p. 1-79, 2009.

BARUH, L.; POPESCU M. Big data analytics and the limits of privacy self-management. **New Media & Society**, Chicago, vol. 19, nº 4, p. 579-96. 2017.

BENKLER, Yochai. **The wealth of networks**: How social production transforms markets and freedom. New Haven, Yale University Press, 2006.

BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. **Network Propaganda**: Manipulation, Disinformation, and Radicalization in American Politics. Oxford. Oxford University Press, 2018.

BERLIN, Isaiah. **Two concepts of liberty**: an inaugural lecture delivered before the university of Oxford. Clarendon, 1959.

BIROLI, F. **Autonomia e desigualdades de gênero**: contribuições do feminismo para a crítica democrática. Niterói: Eduff, 2013.

_____, Flávia. Autonomia, preferências e assimetria de recursos. **Revista Brasileira de Ciências Sociais**, São Paulo, Hucitec v. 31, n. 90, 2016.

BORK, Robert H.; SIDAK, J. Gregory. What Does the Chicago School Teach About Internet Search and the Antitrust Treatment of Google?. Oxford. **Journal of Competition Law and Economics**, v. 8, n. 4, p. 663-700, 2012.

BOURDIEU, Pierre. **A distinção crítica social do julgamento**. São Paulo, Edusp, 2007.

BROWN, Wendy. **Undoing the Demos**: Neoliberalism's Stealth Revolution. New York: Zone Books, 2015.

BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. In: Antoun, Henrique. (Org.). **Web 2.0: Participação e Vigilância na era da comunicação distribuída**. Rio de Janeiro: M53auad X, p. 167-182, 2008.

BUTTS, Chris. The Microsoft Case 10 Years Later: Antitrust and New Leading New Economy Firms. Chicago, **Northwestern Journal of Technology and Intellectual Property.** v. 8, p. 275, 2009.

CASTAÑEDA, Ernesto. The indignados of Spain: A precedent to occupy Wall Street. Londres, **Social Movement Studies**, v. 11, n. 3-4, p. 309-319, 2012.

CAVOUKIAN, Ann. **Privacy by design in law, policy and practice**. A white paper for regulators, decision-makers and policy-makers, Ontario, 2011.

CASTELLS, Manuel et al. **A sociedade em rede**. São Paulo: Paz e Terra, 2001.

COBB, Stephen. Data privacy and data protection: US law and legislation. **An ESET White Paper**, Bratislava, p. 1-15, 2016.

COHEN, Jean. Repensando a privacidade: autonomia, identidade e a controvérsia sobre o aborto. São Paulo, **Revista Brasileira de Ciência Política**, n. 7; pp. 165-203, 2012.

COLEMAN, Stephen; BRUMLER, Jay G. **The Internet and democratic citizenship**: theory, practice and policy. Cambridge: Cambridge University Press, 2009.

DANTAS, Marcos. Convergência digital: entre os "jardins murados" e as praças públicas. **Políticas de comunicacion el capitalismo contemporâneo: América Latina y sus encrucijadas**. Buenos Aires: Consejo Latinoamericano de Ciencias Sociales–CLACSO, 2010.

_____, M. The Financial Logic of Internet Platforms: The Turnover Time of Money at the Limit of Zero. Londres, **Triple C: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society**, v. 17, n. 1, p. 132-158, 2019.
DELEUZE, Gilles. **Conversações**. São Paulo, Editora 34, 1992.
_____, Gilles. **Post-scriptum sobre las sociedades de control**. Santiago, Polis. Revista Latinoamericana, n. 13, 2006.
DELPHY, Christine. The main enemy. **College Park, Feminist Issues**, v. 1, n. 1, p. 23-40, 1980.
DENZIN, Norman K.; LINCOLN, Yvonna S. Thousand Oaks. (Ed.). **The Sage handbook of qualitative research**., 2011.
DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.
DUBY, Georges & ARIÈS, Phillipe. **História da vida privada**. Vol. 1. do Império Romano ao ano mil. São Paulo: Companhia das Letras, 2009.
_____, Georges & ARIÈS, Phillipe. **História da Vida Privada** – Vol 2 Da Europa Feudal à Renascença. São Paulo. Companhia das Letras, 2009.
FERNBACK, Jan; PAPACHARISSI, Zizi. Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. Chicago, **New Media & Society**, v. 9, n. 5, p. 715-734, 2007.
FIALOVÁ, Eva. Data Portability and Informational Self-Determination. **Masaryk UJL & Tech.**, v. 8, p. 45, 2014.
FLUSSER, V. **Filosofia da caixa preta**: ensaios para uma futura filosofia da fotografia. Relume Dumará, 2002.
FRIED, C. **Privacy: A Moral Analysis**. Yale Law Journal 77(1): 475– 493, 1968.
FRIEDMAN, Milton. **The business communitys suicidal impulse**. Cato Policy Report, v. 21, n. 2, p. 6-7, 1999.
FRASER, Nancy. Rethinking the public sphere: a contribution to the critique of actually existing democracy. In: Craig Calhoun (ed.), **Habermas and the public sphere,** The MIT Press, 1992.
_____, Nancy. **Feminism, capitalism, and the cunning of history**. 2012.
FOUCAULT, Michel. **História da sexualidade. v. 1. A vontade de saber**. Rio de Janeiro, Edições Graal, 1988.
_____, Michel. **Vigiar e punir**. Rio de Janeiro, Editora Vozes, 2012.
GAVISON, R. **Privacy and the Limits of the Law**. Yale Law Journal 89: 4 21– 471, 1980.
GOMES, Wilson. Anos de política, estado e democracia digitais: uma cartografia do campo. In **Democracia digital, comunicação política e redes: teoria e prática**, p. 25-45, 2018.
GOMES, W., AMORIM, P. K. D. F., & ALMADA, M. P. (2018). Novos desafios para a ideia de transparência pública. **E-Compós, 21**(2). https://doi.org/10.30962/ec.1446.
HABERMAS, Jürgen. **Mudança estrutural da esfera pública**: investigações quanto a uma categoria da sociedade burguesa. São Paulo: Unesp, 2014.
_____, Jürgen. **Mudança estrutural da esfera pública**: investigações quanto a uma categoria da sociedade burguesa. Rio de Janeiro, Tempo Brasileiro, 1984.
HARVEY, David. **O neoliberalismo**: história e implicações. Loyola, 2008.
HOBBES, T. **Leviatã**, São Paulo: Nova Cultural. 1987.
KANT, I. A **paz perpétua e outros opúsculos**. Lisboa, Edições 70, 2004.
KELLSTEDT, Paul M.; WHITTEN, Guy D. **The fundamentals of political science research**. Cambridge University Press, 2018.
KING, Gary; KEOHANE, Robert O.; VERBA, Sidney. **Designing social inquiry**: Scientific inference in qualitative research. Princeton university press, 1994.
LATOUR, Bruno. **Reagregando o social**: uma introdução à teoria do ator-rede. Edufba, 2012.
LAVAL, Christian; DARDOT, Pierre. **A nova razão do mundo**: ensaios sobre a sociedade neoliberal. São Paulo: Boitempo, 2016.
LIPPMAN, W. **Opinião pública** (Petrópolis, Editora Vozes). 2008.
LYON, David. **The electronic eye**: The rise of surveillance society. U of Minnesota Press, 1994.

_____, David. Surveillance culture: engagement, exposure, and ethics in digital modernity. **International Journal of Communication**, nº 11, pp. 824-42, 2017.
MANIN, B. As metamorfoses do governo representativo. **Revista Brasileira de Ciências Sociais** 10.29, 1995.
MANOVICH, Lev. **The language of new media**. MIT press, 2001.
MARX, Karl; ENGELS, Friedrich. **A ideologia alemã**: crítica da mais recente filosofia alemã em seus representantes. São Paulo. Boitempo, 2007.
MCLUHAN, Marshall. **Os meios de comunicação**: como extensões do homem. Editora Cultrix, 1974.
MEIRELES, Adriana Veloso. **Democracia 3.0: interação entre governo e cidadãos mediada por tecnologias digitais**. Dissertação (Mestrado em Design)—Universidade de Brasília, 2015.
MIGUEL, Luis Felipe. **Dominação e resistência**: desafios para uma política emancipatória. São Paulo: Boitempo Editorial. 200Pp, 2018.
_____, Luis Felipe. **Democracia e representação: territórios em disputa**. Editora Unesp, 2014.
_____, Luis. Felipe. (2015). Autonomia, paternalismo e dominação na formação das preferências. **Opinião Pública**, *21*(3), 601-625. 2015
MILL, Stuart. **O governo representativo**. São Paulo, Ibrasa, 1995.
MILNER, Ryan M. Pop polyvocality: Internet memes, public participation, and the Occupy Wall Street movement. **International Journal of Communication**, v. 7, p. 34, 2013.
MOUFFE, Chantal. Por um modelo agonístico de democracia. **Revista de Sociologia e Política**, Curitiba, v. 25, p. 11-23, nov. 2005.
MOGGRIDGE, B. **Designing Interactions**. Massachusetts: MIT Press. 2006.
MOVIUS, Lauren B.; KRUP, Nathalie. US and EU privacy policy: comparison of regulatory approaches. **International Journal of Communication**, v. 3, p. 19, 2009.
NIELSEN, J. **Usability Engineering**. San Francisco: Morgan Kaufmann Publishers. 1994
NISSENBAUM, H. **Privacy in context: Technology, policy and the integrity of social life**. Stanford, CA: Stanford University Press, 2009.
NORMAN, Donald. **Design Emocional**. Rio de Janeiro: Rocco, 2008.
O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. Broadway Books, 2016.
OKIN, Susan Moller. Gênero, o público e o privado. **Revista Estudos Feministas**, n. 16, vol. 2, pp. 305-332, 2008.
PAGE, Lawrence, BRIN, Sergey. The anatomy of a large-scale hypertextual web search engine. **Computer networks and ISDN systems**, v. 30, n. 1-7, p. 107-117, 1998.
PARISER, Eli. **The filter bubble**: What the Internet is hiding from you. Penguin UK, 2011.
PAPACHARISSI, Zizi. **Affective publics**: Sentiment, technology, and politics. Oxford University Press, 2015.
_____, Zizi. **A private sphere**: Democracy in a digital age. Polity, 2010.
PATEMAN, Carole. **O contrato sexual.** Rio de Janeiro: Paz e Terra, 1993.
_____, Carole. Críticas feministas à dicotomia público privado. Em **Teoria política feminista: textos centrais**, Niterói, Eduff,. pp. 55-80, 2013.
PETTIT, Philip. **Republicanism: a theory of freedom and government.** OUP Oxford, 1997.
PHILLIPS, Anne. O que há de errado com a democracia liberal?. **Revista Brasileira de Ciência Política**, n. 6, pp. 339-363, 2011.
PITKIN, Hanna Fenichel. Are freedom and liberty twins?. **Political Theory**, v. 16, n. 4, p. 523-552, 1988.
PREECE, J.; ROGERS, Y; SHARP, H. **Design de Interação: além da interação homem-computador**. Porto Alegre: Bookman, 2005.
REGAN, P . **Legislating Privacy**. Chapel Hill: University of North Carolina Press, 1995.
SAFFER, Dan. **Designing for interaction**: creating innovative applications and devices. New Riders, 2010.

SAMPAIO, R.; BRAGATTO, R.; NICOLÁS, M. Inovadora e democrática. Mas e aí? Uma análise da primeira fase da consulta online sobre o Marco Civil da Internet.In: **V Congresso da Compolítica**: Curitiba. 2013. p. 01-31.
SANTARÉM, P. R. S. **O direito achado na rede**: a emergência do acesso à Internet como direito fundamental no Brasil. 2010. 158 f., il. Dissertação (Mestrado em Direito, Estado e Constituição)-Universidade de Brasília, Brasília, 2010.
SAXONHOUSE, Arlene. Classical greek conceptions of public and private. In: BENN, S.I; GAUS, G.F. (Org). **Public and Private in Social Life**. Nova York: St. Martins Press. p. 363-384, 1983.
SCHUMPETER, J. **Capitalism, Socialism and Democracy**. Londres: Allen and Unwin, 1976.
SCOTT, J. **Domination and the arts of resistance**: Hidden transcripts. Estados Unidos. Yale university Press, 1990.
SILVEIRA, Sérgio Amadeu. Economia da intrusão e modulação na internet. **Liinc em Revista**, v. 12, n. 1, 2016.
_____, Sérgio Amadeu. **Tudo sobre Tod@s**: Redes Digitais, Privacidade e Venda de Dados Pessoais. São Paulo: Edições Sesc São Paulo, 2017.
SILVA, Sivaldo Pereira da. Transparência digital em instituições democráticas; horizontes, limites e barreiras. In: MENDONÇA, Ricardo Fabrino; PEREIRA, Marcus Abílio; FILGEIRAS, Fernando (Org.). **Democracia digital: Publicidade, instituições e confronto político**. Belo Horizonte: Editora UFMG, p. 27-53-. 2016
SNOWDEN, Edward. **Permanent Record**. Metropolitan Books; 1st Edition edition, 2019)
SOLAGNA, F. **A formulação da agenda e o ativismo em torno do Marco Civil da Internet**. Dissertação (Mestrado) Universidade Federal do Rio Grande do Sul, Instituto de Filosofia e Ciências Humanas, Programa de Pós-Graduação em Sociologia, Porto Alegre, BR-RS, 2015.
STALLINGS, William. **Criptografia e segurança de redes**, tradução Vieira, Daniel. 2008.
SUNSTEIN, Cass. R. Preferências e política. **Revista Brasileira de Ciência Política**, no 1, pp. 219-54, 2009.
_____, Cass R. **Republic. com**. Princeton university press, 2002.
TIEN, J. M. Big data: unleashing information. **Journal of Systems Science and Systems Engineering**, vol. 22, nº 2, pp. 127-51. 2013.
TUTT, Andrew, An FDA for Algorithms. **Admin. L. Rev**. 83, 2017.
VAN DEN HOVEN, Jeroen. **Privacy and the varieties of informational wrongdoing**. 1999.
VON BÜLOW, Marisa; PONTE, Germán Bidegain. It takes two to tango: Students, political parties, and protest in Chile (2005–2013). In: **Handbook of social movements across Latin America**. Springer, Dordrecht, p. 179-194, 2015.
WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard law review**, p. 193-220, 1890.
WEBER, Max **Economia e sociedade**, vol. 1. Brasília: Editora UnB, 1991.
WEINTRAUB, Jeff. The theory and politics of the public/private distinction. **Public and private in thought and practice**: Perspectives on a grand dichotomy, Chicago, Chicago Press Books, v. 1, p. 7, 1997.
WOLF, Mauro. **Teorias das comunicações de massa**. São Paulo: Martins Fontes, 2005.
WOOD, Ellen Meiksins. **Democracia contra capitalismo: a renovação do materialismo histórico.** São Paulo, Boitempo, 2003.
YOUNG, Iris. **Justice and the Politics of Difference.** Princeton: Princeton University Press, 1990.
ZUBOFF, Shoshana. **The age of surveillance capitalism: The fight for a human future at the new frontier of power**. Londres, Profile Books, 2019.

Anexo 1: Dados agrupados

privacy	security	surveillance	rights	freedom	Ano	Sessão
1	14	0	16	11	2006	IGF-OpeningSession-301006
0	2	0	1	7	2006	IGF-Panel5-Access
0	6	0	4	0	2006	IGF-SummingUp-011106
0	1	0	7	6	2006	IGF-Panel6-Emerging Issues
0	9	0	8	4	2006	IGF-Closing%20Ceremony
1	26	0	6	2	2006	IGF-Panel1setting the scene
1	28	1	11	15	2006	IGF-Summing_Up_Nov_1
2	15	3	95	71	2006	IGF-Panel2-Openness
3	3	0	20	8	2006	IGF-Summing_Up_Nov_2
11	37	1	16	21	2006	IGF-SummingUp2-021106am
26	191	2	5	1	2006	IGF-Panel3-Security
1	13	0	0	0	2007	IGF2-Critical%20Internet%20Resources-12NOV07
0	0	0	3	1	2007	IGF2-Access-13NOV07
0	0	0	0	0	2007	IGF2-ReportingBack-Afternoon-13NOV07
0	2	0	1	1	2007	IGF2-opening-12NOV07
0	1	0	1	0	2007	IGF2-ReportingBack-Morning-13NOV07
0	0	0	7	7	2007	IGF2-Diversity-13NOV07
2	6	0	1	2	2007	IGF2-Closing-15NOV07
2	20	0	34	17	2007	IGF_opening_Session
3	1	0	14	10	2007	IGF2-EmergingIssues-15NOV07
4	5	0	7	6	2007	IGF2-TakingStock-15NOV07
4	13	0	11	28	2007	IGF2-ReportingBack-Morning-14NOV07
15	15	0	19	5	2007	IGF2-ReportingBack-15NOV07
17	154	3	10	2	2007	IGF2-Security-14NOV07
24	4	2	86	75	2007	IGF2-Openness-14NOV07
0	9	0	0	0	2008	Transition from IPv4 to IPv6

0	0	0	0	0	2008	Open Dialogue
0	14	0	0	0	2008	Arrangements for Internet Governance, Global and National Regional.txt
0	1	0	1	0	2008	Realizing a Multilingual Internet
0	1	0	1	0	2008	access
0	4	0	2	1	2008	Opening Ceremony
1	14	0	0	2	2008	Open Dialogue 3
3	12	0	4	1	2008	Closing ceremony
6	17	0	4	8	2008	Opening Session
6	74	0	5	1	2008	Dimensions of cyber-security and cyber-crime
32	19	0	28	3	2008	Taking Stock and the Way Forward
36	35	0	59	7	2008	The Internet of Tomorrow Innovation and the Evolution of the Internet
45	39	1	37	15	2008	Fostering Security, Privacy, and Openness.txt
78	100	0	52	25	2008	Open Dialogue 2
152	90	2	83	26	2009	Security, Openness and Privacy.txt
0	5	0	7	1	2009	Access
0	2	0	8	4	2009	Diversity
1	3	0	13	24	2009	Opening Session
2	6	0	7	2	2009	Orientation Session
3	6	0	1	5	2009	Taking Stock Part 1
3	5	0	3	5	2009	Opening Ceremony
4	7	0	1	2	2009	Critical Internet Resources
4	9	0	4	1	2009	Closing Ceremony
5	2	0	21	3	2009	Emerging Issues - Impact of Social Networks
6	8	0	3	3	2009	Taking Stock Part 2
6	7	0	26	9	2009	IG in the Light of WSIS Principles
7	8	0	14	1	2009	Honourary Session

13	19	0	4	3	2009	Regional Perspectives
7	7	1	13	4	2010	644-access-and-diversity
4	10	0	1	0	2010	643-resources
4	2	0	1	0	2010	688-closing-ceremony
4	8	0	4	10	2010	665-ig4dEVELOPMENT
7	10	0	16	12	2010	687-taking-stock
8	8	0	16	2	2010	627-regional
10	27	0	8	8	2010	626-scene
16	27	0	28	26	2010	628-opening-cereminy
30	34	0	4	1	2010	674-cloud
93	97	0	65	54	2010	658-SECURITY, OPENNESS AND PRIVACY.html
3	3	0	2	2	2011	863-main-session-critical-internet-resources
4	3	0	8	0	2011	864-main-session-taking-stock-and-the-way-forward
4	2	0	29	9	2011	861-main-session-access-and-diversity
5	19	0	1	4	2011	859-opening-ceremony
5	5	0	3	0	2011	858-opening-ceremony
7	11	0	14	16	2011	857-main-session-internet-governance-for-development
10	10	0	23	6	2011	856-main-session-internet-governance-for-development
22	26	0	4	8	2011	860-inter-regional-dialogue
78	114	7	57	39	2011	862-main-session-secuirt-openness-and-privacy
8	20	1	22	27	2012	Opening Ceremony and Opening Session
4	1	1	3	0	2012	1251-igf-2012-internet-governance-for-development-main-session
4	6	0	7	4	2012	1260-igf-2012-closing-ceremony-
4	4	0	50	15	2012	1258-igf-2012-access-and-

						diversity-main-session
5	3	1	15	3	2012	1250-igf-2012-management-of-critical-internet-resources-main-session
5	5	0	24	27	2012	1254-igf-2012-emerging-issues-main-session
17	16	4	59	25	2012	1259-igf-2012-taking-stock-and-the-way-forward-main-session
72	84	14	85	75	2012	1256-igf-2012-security-openness-privacy
13	9	2	72	19	2013	1451-focus-session-internet-governance-principles
2	0	0	1	0	2013	1452-focus-session-principles-of-multi-stakeholder-cooperation
2	3	2	1	1	2013	1408-focus-session-accessdiversity-internet-as-an-engine-for-growth-and-sustainable-development-icts-and-development-in-the-real-world-concrete-experiences-of-how-internet-governance-has-impacted-development
3	6	3	3	0	2013	1458-closing-ceremony
4	4	6	38	12	2013	1447-building-bridges-the-role-of-governments-in-multistakeholder-cooperation
11	79	2	6	2	2013	1401-focus-session-security-legal-and-other-frameworks-spam-hacking-and-cybercrime
17	36	9	22	17	2013	1375-opening-ceremony-and-opening-session
33	11	64	138	127	2013	1421-focus-session-openness-human-rights-freedom-of-expression-and-free-flow-of-

						information-on-the-internet
49	68	87	125	28	2013	1439-taking-stock-emerging-issues-internet-surveillance
2	10	0	2	0	2014	FINISHED - 2014 09 04 - Best Practice Forums Wrap Up - Main Room
2	7	0	3	1	2014	2019-2014-09-05-ms-iana-functions-main-hall
2	1	1	6	0	2014	2101-finished-2014-09-02-orientation
3	0	0	3	5	2014	FINISHED - 2014 09 04 - WS173 - Youth involvement in Internet Governance - Main Hall
3	1	0	8	5	2014	1949-2014-09-03-policies-enabling-access-main-room
6	2	1	17	0	2014	2020-2014-09-05-taking-stock-emerging-issues-main-hall
6	3	3	38	2	2014	1928-2014-09-02-topical-insight-main-hall
6	2	0	43	41	2014	1996-2014-09-03-towards-a-common-understanding-of-network-neutrality-main-hall
7	18	8	10	1	2014	1977-2014-09-04-ms-evolution-of-the-ig-main-room
8	7	3	12	1	2014	FINISHED - 2014 09 05 - Closing Ceremony - Anadolu Auditorium
12	8	5	11	14	2014	FINISHED - 2014 09 05 - Open microphone session - Anadolu Auditorium
14	11	0	14	7	2014	FINISHED - 2014 09 02 - Opening Ceremony_Opening Session - Anadolu Auditorium
6	1	0	22	15	2015	2984-2015-11-13-dynamic-coalitions-feedback-main-

						meeting-room-finished
50	17	10	177	56	2015	2985-2015-11-13-human-rights-on-the-internet-main-meeting-room-finished
3	1	2	11	14	2015	2015 11 13 Open Mic Main Meeting Hall FINISHED
4	7	1	17	4	2015	2854-2015-11-11-internet-economy-and-sustainable-development-main-meeting-hall
5	1	2	18	18	2015	2874-2015-11-12-a-dialogue-on-zero-rating-and-network-neutrality-main-meeting-room-finished
6	224	7	26	7	2015	2884-2015-11-12-enhancing-cybersecurity-and-building-digital-trust-main-meeting-hall-finished
8	16	6	10	16	2015	2824-2015-11-10-setting-the-scene-workshop-room-11
8	7	0	17	21	2015	2015 11 13 Closing Ceremony Main Meeting Hall FINISHED
9	1	1	38	7	2015	2872-2015-11-12-main-session-on-dynamic-coalitions-main-meeting-room-finished
10	13	1	19	7	2015	2853-2015-11-11-igf-intersessional-work-policy-options-and-best-practices-for-connecting-the-next-billion-main-meeting-hall
10	31	6	38	4	2015	2834-2015-11-10-wsis-10-consultations-main-meeting-hall
11	31	7	28	5	2015	2987-2015-11-13-the-netmundial-statement-and-the-evolution-of-the-internet-governance-

						ecosystem-main-meeting-hall-finished
20	17	2	35	19	2015	2836-2015-11-10-opening-session-main-meeting-hall
9	15	5	25	6	2016	igf-2016-day-1-main-hall-setting-the-scene-orientation-opening-ceremony-opening-session
2	4	0	7	1	2016	igf-2016-day-4-main-hall-shaping-the-future-of-internet-governance
3	5	0	9	0	2016	igf-2016-day-4-main-hall-closing-ceremony
4	5	0	2	4	2016	igf-2016-day-1-main-hall-assessing-the-role-of-ig-in-the-sdgs
4	20	0	5	1	2016	igf-2016-day-4-main-hall-igf-bpfs-and-policy-options-for-connecting-the-next-billions
4	4	0	8	2	2016	igf-2016-day-1-main-hall-setting-the-scene-orientation-opening-ceremony
4	8	0	26	0	2016	igf-2016-day-3-main-hall-igf-dynamic-coalitions
5	5	1	6	9	2016	igf-2016-day-2-main-hall-sustainable-development-internet-and-inclusive-growth
8	18	0	19	2	2016	igf-2016-day-3-main-hall-trade-agreements-and-the-internet
13	34	7	15	4	2016	igf-2016-day-2-main-hall-national-and-regional-igfs
36	9	17	305	51	2016	igf-2016-day-3-main-hall-human-rights-broadening-the-conversation
17	11	1	3	1	2017	igf-2017-day-4-room-xvii-digital-

						transformation-how-do-we-shape-its-socioeconomic-and-labor
2	4	0	54	11	2017	igf-2017-day-3-room-xvii-plenary-gender-inclusion-the-future-of-the-internet
3	9	0	2	2	2017	igf-2017-day-4-assembly-hall-closing-ceremony
3	23	0	13	6	2017	igf-2017-day-1-assembly-hall-high-level-thematic-session-shaping-our-future-digital-global
3	5	0	55	11	2017	igf-2017-day-3-room-xvii-plenary-nri-perspectives-rights-in-the-digital-world-2nd-section
4	7	1	7	1	2017	igf-2017-day-1-assembly-hall-opening-ceremony
5	19	2	8	8	2017	igf-2017-day-4-assembly-hall-open-mic
5	206	2	23	6	2017	igf-2017-day-2-room-xvii-plenary-empowering-global-cooperation-on-cybersecurity-for
6	5	0	20	9	2017	igf-2017-day-3-room-xvii-dynamic-coalitions-contribute-to-the-digital-future
9	10	1	20	19	2017	igf-2017-day-2-room-xvii-plenary-high-level-thematic-session-impact-of-digitization-on
13	14	5	105	5	2017	igf-2017-day-3-room-xvii-plenary-nri-perspectives-rights-in-the-digital-world
22	59	9	41	13	2017	igf-2017-day-1-room-xvii-plenary-local-interventions-global-impacts-how-can-international
12	7	0	1	1	2018	Salle I - EMERGING

						TECHNOLOGIES
0	2	0	2	0	2018	IGF 2018 - Day 1 - Salle I - High Level Panel Discussion: Strengthening the Internet Governance and the IGF
7	6	0	0	1	2018	IGF 2018 - Day 1 - Salle I - High Level Panel Discussion: The New Challenges of the Internet Governance
0	3	0	2	28	2018	Salle I - MEDIA & CONTENT
16	73	0	21	10	2018	Salle I - CYBERSECURITY, TRUST & PRIVACY
3	7	0	15	1	2018	Salle I - DEVELOPMENT, INNOVATION AND ECONOMIC ISSUES
3	5	0	1	1	2018	Salle I - EVOLUTION OF INTERNET GOVERNANCE
2	4	0	57	12	2018	Salle I - HUMAN RIGHTS, GENDER AND YOUTH
0	0	0	1	1	2018	Salle I - DIGITAL INCLUSION & ACCESSIBILITY
3	4	1	6	14	2018	Salle I - TECHNICAL & OPERATIONAL TOPICS
3	10	1	13	4	2018	Salle I - OPENING CEREMONY
6	15	4	20	13	2018	IGF 2018 - Day 3 - Salle I - OPEN MIC/TAKING STOCK
1	4	0	6	2	2018	Day 3 - Salle I - CLOSING CEREMONY
0	2	0	2	0	2019	IGF For Beginners Main Session
1	4	1	10	13	2019	Day 1 – Convention Hall II – Opening Ceremony
3	2	0	2	0	2019	Day 1 – Convention Hall II – High Level Session on SMEs and Internel Governance

1	6	0	12	2	2109	Day 1 – Convention Hall II – High Level Session on the Future of Internet Governance
3	1	0	79	2	2109	IGF 2019 – Day 2 – Convention Hall II – Applying human rights and ethics in responsible data governance and AI
4	7	3	36	28	2109	IGF 2019 – Day 2 – Convention Hall II – Addressing Terrorist and Violent Extremist Content Online
9	8	0	33	4	2109	Achieving the SDGs in the Digital Age
18	45	2	22	1	2109	IGF 2019 – Day 3 – Convention Hall II – Emerging technologies and their interfaces with inclusion, security and human rights (NRIs)
5	16	4	30	16	2109	IGF 2019 – Day 4 – Convention Hall II – Legislative Main Session
2	19	4	31	11	2109	IGF 2019 – Day 4 – Convention Hall II – Bringing it all together and Open Mic/Taking Stock
1	3	0	1	8	2109	IGF 2019 – Day 4 – Convention Hall II – Closing Ceremony
1612	**3049**	**356**	**3543**	**1650**		**TOTAL**