UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE FILOSOFIA E CIÊNCIAS HUMANAS

JÚLIA TIBIRIÇÁ DIEGUES GOMES

OS TERMOS DE PRIVACIDADE FORAM ATUALIZADOS: REGULAÇÃO E PRODUÇÃO DE SUBJETIVIDADES NA GOVERNANÇA GLOBAL DA INFORMAÇÃO

CAMPINAS

2025

JÚLIA TIBIRIÇÁ DIEGUES GOMES

OS TERMOS DE PRIVACIDADE FORAM ATUALIZADOS: REGULAÇÃO E PRODUÇÃO DE SUBJETIVIDADES NA GOVERNANÇA GLOBAL DA INFORMAÇÃO

Tese apresentada ao Instituto de Filosofia e Ciências Humanas da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Relações Internacionais, na área de concentração Instituições, Processos e Atores.

Orientador: Prof Dr. Eduardo Barros Mariutti

ESTE TRABALHO CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELA ALUNA JÚLIA TIBIRIÇÁ DIEGUES, E ORIENTADA PELO PROF. DR. EDUARDO BARROS MARIUTTI.

CAMPINAS

2025

Ficha catalográfica
Universidade Estadual de Campinas (UNICAMP)
Biblioteca do Instituto de Filosofia e Ciências Humanas
Neiva Goncalves de Oliveira - CRB 8/6792

Gomes, Júlia Tibiriçá Diegues, 1992-
G585t Os termos de privacidade foram atualizados : regulação e produção de subjetividades na governança global da informação / Júlia Tibiriçá Diegues Gomes. – Campinas, SP : [s.n.], 2025.

Orientador: Eduardo Barros Mariutti.
Tese (doutorado) – Universidade Estadual de Campinas (UNICAMP), Instituto de Filosofia e Ciências Humanas.

1. Proteção de dados. 2. Privacidade. 3. Neoliberalismo. 4. Governança da Internet. 5. Vigilância eletrônica. I. Mariutti, Eduardo Barros, 1974-. II. Universidade Estadual de Campinas (UNICAMP). Instituto de Filosofia e Ciências Humanas. III. Título.

Informações complementares

Título em outro idioma: The privacy policy has been updated : regulation and production of subjectivities in global information governance
Palavras-chave em inglês:
Data protection
Privacy
Neoliberalism
Internet governance
Electronic surveillance
Área de concentração: Instituições, Processos e Atores
Titulação: Doutora em Relações Internacionais
Banca examinadora:
Eduardo Barros Mariutti [Orientador]
Alana Moraes de Souza
Acácio Augusto Sebastião Junior
Jean François Germain Tible
Carlos Alberto Cordovano Vieira
Data de defesa: 15-12-2025
Programa de Pós-Graduação: Relações Internacionais

Objetivos de Desenvolvimento Sustentável (ODS)
Não se aplica

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0001-7866-1456
- Currículo Lattes do autor: http://lattes.cnpq.br/7137099912610294

IMPACTO POTENCIAL DESTA PESQUISA

Esta pesquisa contribui para a compreensão contemporânea das relações entre privacidade, vigilância e governamentalidade no contexto internacional e brasileiro, oferecendo subsídios analíticos para formulação de políticas públicas, aprimoramento regulatório e capacitação institucional em proteção de dados.

POTENTIAL IMPACT OF THIS RESEARCH

This research advances the critical understanding of the relations between privacy, surveillance and governmentality in Brazilian and international contexts, providing analytical support for public policy design, regulatory improvement and institutional capacity-building in data protection.

IMPACTO POTENCIAL DE ESTA INVESTIGACIÓN

Esta investigación contribuye a la comprensión crítica de las relaciones entre privacidad, vigilancia y gubernamentalidad en los contextos brasileño e internacional, aportando insumos analíticos para el diseño de políticas públicas, el perfeccionamiento regulatorio y el fortalecimiento institucional en protección de datos.

Profa. Dra. Alana Moraes de Souza

Prof. Dr. Jean François Germain Tible

Prof. Dr. Acácio Augusto Sebastião Junior

Prof. Dr. Carlos Alberto Cordovano Vieira

A Ata de Defesa com as respectivas assinaturas dos membros encontra-se no SIGA/Sistema de Fluxo de Dissertações/Teses e na Secretaria do Programa de Pós-Graduação em Relações Internacionais do Instituto de Filosofia e Ciências Humanas.

Para Tío Dino, que me enseñó, en un sobresalto,

"de la implacable sensación de que mi vida se me queda corta"

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. As opiniões, hipóteses e conclusões ou recomendações aqui expressas são de responsabilidade dos autores e não necessariamente refletem a visão da CAPES. O apoio foi concedido entre agosto de 2021 e fevereiro de 2024, pelo processo nº 88887.634403/2021-00 e entre janeiro de 2023 e maio de 2023, pelo processo nº 88881.676782/2022-01, por meio do Edital 14/2021. Agradeço a CAPES pelo apoio concedido, tal como ao PROPEX-DEFESA, pela oportunidade de período sanduíche no exterior.

Agradeço ao Prof. Dr. Eduardo Mariutti pela confiança e inspiração.

Agradeço ao Prof. Dr. David Murakami Wood, pela generosidade e atenção, durante meu período na Universidade de Ottawa.

Agradeço aos funcionários do Programa San Tiago Dantas pela impecável presteza.

Agradeço aos membros da banca pela leitura e oportunidade de diálogo.

Agradeço ao LASInTec, pelos impulsos libertários. Agradeço a Faculdade Latino Americana de Ciências Sociais, pelas empreitadas sempre desafiadoras, e as Faculdades Metropolitanas Unidas, sobretudo ao Prof. Thiago Matiolli, pela parceria e escuta, regadas a capuccino. Um agradecimento especial a Andrea Azevedo, a amiga-irmã da década que esteve - de perto ou de longe - sempre junto para compartilhar e - às vezes - interromper delírios megalomaníacos em torno deste projeto, e outros mais.

Ao Guilherme e à Elvira, pelo companheirismo, pelas aventuras e desventuras vividas, pelo apoio - por tantos apoios, sem os quais verdadeiramente nada teria sido possível nesse percurso. Ao Buba, Panqueca e Nacho, pela presença alentadora. Ao meu pai, pelos jantares que me deram sustança — corpo e fôlego — enquanto eu tocava este projeto.

À Andrea, ao Bruno, à Alice e Raquel, por fazer dos meus tempos em Ottawa repletos de sons, carinhos e gostos de Brasil. Ao *Center for Law, Society and Technology*, ao Matheus e à Anna, que enfrentaram comigo o inverno inamistoso da cidade (e, às vezes, da pesquisa). À Helena, pelas coincidências de percurso.

Ao Kevin, um agradecimento mais do que especial, pela grata grande surpresa que o Canadá me deu. Eu sei que a reta final deste processo não trouxe à tona a melhor versão de mim (mas ela virá!) - obrigada pela paciência e carinho.

Há um último agradecimento difícil de pôr em palavras.

Quando eu estava na segunda ou terceira série, uma atividade da escola nos pedia responder o que queríamos ser quando crescessemos. Primeiro, respondi que queria ser a minha mãe. Depois, mudei de ideia, e optei pelo Indiana Jones. Na noite do 14 de Agosto de 2023 entrei pela primeira vez em uma sala de aula *minha*, depois de décadas performando o papel de aluna. Não foi um encontro fácil. Era uma sala lotada de corpos desobedientes, inquietos, entediados, e eu não sabia, de jeito nenhum, o que fazer com eles. E no dia seguinte, de novo. E de novo.

Minha mãe é professora (anos depois da segunda série eu perceberia que Indiana Jones também era!) Ao longo do tempo, tive evidências de sobra que poderiam ter me dissuadido de seguir o mesmo caminho: o sobretrabalho - principalmente extraclasse -, a falta de reconhecimento, as pilhas de coisas para corrigir, a voz que some ao final do semestre, a rotina exaustiva, os horários ingratos, as crises existenciais-cotidianas com a educação superior, enfim. Eu não acho que minha mãe queria que eu fosse professora. Eu entendo. É um tipo de vínculo que é como um vício, um amor tóxico — do qual ela preferiria me ver livre, embora ela mesma jamais tenha conseguido escapar. Ainda bem.

Pouco mais de 2 anos depois daquele 14 de Agosto, sigo sistematicamente retornando a bell hooks seja nos dias de fúria ou de profundo encantamento, já que ela tão bem traduz algumas das percepções que só conseguimos, de fato, ter lá, ao performar "o outro lado" do espetáculo: "*a sala de aula continua sendo o espaço de possibilidade mais radical na academia"* (hooks, 2013, p. 23). Meus agradecimentos finais, e talvez mais importantes, vão para minhas alunas e alunos, que me confirmam essa constatação todos os dias, mesmo nos mais improváveis e que me levaram a perceber que eu tinha, talvez, finalmente absoluta clareza sobre os maiores amores da minha vida: a sala de aula, e a minha mãe. Será a maior honra, eu descobri, se quando eu crescer eu me tornar metade da professora que ela é. Obrigada, mãe. A docência é um presente.

no matter how paranoid you are, you're not paranoid enough

Arquivo X (1997)

RESUMO

A privacidade está em crise. Trata-se do diagnóstico recorrente no debate contemporâneo sobre segurança e governança digital, especialmente diante da centralidade assumida pela circulação de dados em sociedades cibermediadas. Frequentemente se presume que a expansão das tecnologias computacionais e a crescente mercantilização da informação teriam corroído, de modo irreversível, a esfera da "vida privada" e das "informações pessoais". Este trabalho, no entanto, busca problematizar tal formulação linear, examinando como a privacidade em sua formulação contemporânea opera como dispositivo de governo. O argumento desenvolvido evidencia que, mais do que simples erosão, trata-se de uma reconfiguração: as políticas e práticas de segurança da informação convocam determinadas concepções de privacidade, frequentemente minimalistas ou incoerentes com o regime sociotécnico vigente, ao mesmo tempo em que ocultam dimensões estruturais da captura e da vigilância. Nesse sentido, a investigação se encerra no processo de institucionalização da proteção de dados pessoais e da privacidade no Brasil, situando a emergência de marcos regulatórios como o Marco Civil da Internet e a Lei Geral de Proteção de Dados em um horizonte marcado pela circulação transnacional de modelos normativos, pela pressão de mercados digitais globais e pela crescente centralidade da privacidade como condição de legitimidade no plano internacional. A partir de uma leitura genealógica, buscou-se compreender como tais instrumentos jurídicos participam da consolidação de racionalidades neoliberais e securitárias que associam privacidade à gestão de riscos e à responsabilização individual. Dessa forma, nossa pesquisa procurou mostrar como essa tensão é mobilizada para estruturar formas específicas de governamentalidade digital, problematizando a forma como os discursos sobre a privacidade são articulados, esvaziados ou instrumentalizados, e procurando identificar tanto os limites das concepções dominantes quanto as fissuras a partir das quais emergem alternativas tecnopolíticas. Assim, a privacidade aparece não como categoria em dissolução, mas como campo de disputa, cujas múltiplas definições e apropriações refletem a ambivalência de democracias contemporâneas profundamente marcadas por práticas de vigilância, regulação econômica e disputas por soberania informacional.

Palavras-chave: proteção de dados; privacidade; vigilância; neoliberalismo; governança da internet

ABSTRACT

Privacy is in crisis. This is the recurrent diagnosis in contemporary debates on security and digital governance, especially in light of the centrality assumed by the circulation of data in cyber-mediated societies. It is often presumed that the expansion of computational technologies and the growing commodification of information have irreversibly eroded the sphere of "private life" and "personal information." This work, however, seeks to problematize such a linear formulation, examining how privacy in its contemporary formulation operates as a device of government. The argument developed shows that, more than a simple erosion, it is a reconfiguration: information security policies and practices summon certain conceptions of privacy, often minimalist or incoherent with the prevailing socio-technical regime, while simultaneously concealing structural dimensions of capture and surveillance. In this sense, our investigation focuses on the process of institutionalization of personal data protection and privacy in Brazil, situating the emergence of regulatory frameworks such as the *Marco Civil da Internet* and the *Lei Geral de Proteção de Dados* within a horizon marked by the transnational circulation of normative models, the pressure of global digital markets, and the growing centrality of privacy as a condition of legitimacy in the international arena. From a genealogical reading, the aim was to understand how such legal instruments participate in the consolidation of neoliberal and securitarian rationalities that associate privacy with risk management and individual responsibility. Thus, our research sought to show how this tension is mobilized to structure specific forms of digital governmentality, problematizing the way in which discourses on privacy are articulated, emptied, or instrumentalized, and seeking to identify both the limits of dominant conceptions and the fissures from which techno-political alternatives emerge. Privacy therefore appears not as a category in dissolution, but as a field of dispute, whose multiple definitions and appropriations reflect the ambivalence of contemporary democracies deeply marked by practices of surveillance, economic regulation, and disputes over informational sovereignty.

Key words: privacy; surveillance; neoliberalism; internet governance

RESUMEN

La privacidad está en crisis. Se trata del diagnóstico recurrente en el debate contemporáneo sobre seguridad y gobernanza digital, especialmente ante la centralidad asumida por la circulación de datos en sociedades cibermediadas. Frecuentemente se presume que la expansión de las tecnologías computacionales y la creciente mercantilización de la información habrían corroído, de modo irreversible, la esfera de la "vida privada" y de las "informaciones personales". Este trabajo, sin embargo, busca problematizar tal formulación lineal, examinando cómo la privacidad en su formulación contemporánea opera como dispositivo de gobierno. El argumento desarrollado evidencia que, más que una simple erosión, se trata de una reconfiguración: las políticas y prácticas de seguridad de la información convocan determinadas concepciones de privacidad, frecuentemente minimalistas o incoherentes con el régimen sociotécnico vigente, al mismo tiempo que ocultan dimensiones estructurales de la captura y de la vigilancia. En este sentido, la investigación se centra en el proceso de institucionalización de la protección de datos personales y de la privacidad en Brasil, situando la emergencia de marcos regulatorios como el *Marco Civil de Internet* y la *Ley General de Protección de Datos Personales* en un horizonte marcado por la circulación transnacional de modelos normativos, por la presión de los mercados digitales globales y por la creciente centralidad de la privacidad como condición de legitimidad en el plano internacional. A partir de una lectura genealógica, se buscó comprender cómo tales instrumentos jurídicos participan en la consolidación de racionalidades neoliberales y securitarias que asocian la privacidad a la gestión de riesgos y a la responsabilización individual. De esta forma, nuestra investigación procuró mostrar cómo esa tensión es movilizada para estructurar formas específicas de gubernamentalidad digital, problematizando la manera en que los discursos sobre la privacidad son articulados, vaciados o instrumentalizados, y buscando identificar tanto los límites de las concepciones dominantes como las fisuras a partir de las cuales emergen alternativas tecnopolíticas. Así, la privacidad aparece no como categoría en disolución, sino como un campo de disputa, cuyas múltiples definiciones y apropiaciones reflejan la ambivalencia de las democracias contemporáneas profundamente marcadas por prácticas de vigilancia, regulación económica y disputas por soberanía informacional.

Palabras clave: protección de datos; privacidad; vigilancia; neoliberalismo; gobernanza de internet

LISTA DE ABREVIATURAS E SIGLAS

ABIN – Agência Brasileira de Inteligência
ACP – Ação Civil Pública
AGNU – Assembleia Geral das Nações Unidas
ANPD – Autoridade Nacional de Proteção de Dados
APEC – Asia-Pacific Economic Cooperation
CDC – Código de Defesa do Consumidor
CDCiber – Centro de Defesa Cibernética
CICC – Centros Integrados de Comando e Controle
ComDCiber – Comando de Defesa Cibernética
CPI – Comissão Parlamentar de Inquérito
EC – Emenda Constitucional
E-Ciber – Estratégia Nacional de Segurança Cibernética
GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados – União Europeia)
GSI-PR – Gabinete de Segurança Institucional da Presidência da República
HIPAA – Health Insurance Portability and Accountability Act (EUA)
IGF – Internet Governance Forum
LAI – Lei de Acesso à Informação
LGPD – Lei Geral de Proteção de Dados Pessoais
MCI – Marco Civil da Internet
MP – Medida Provisória
NSA – National Security Agency (EUA)
OCDE – Organização para a Cooperação e Desenvolvimento Econômico
OHCHR – Office of the High Commissioner for Human Rights (ACNUDH)
ONU – Organização das Nações Unidas
PEC – Proposta de Emenda à Constituição
PNSI – Política Nacional de Segurança da Informação
PPSI – Programa de Privacidade e Segurança da Informação

RIPD – Red Iberoamericana de Protección de Datos

SNI – Serviço Nacional de Informações

STF – Supremo Tribunal Federal

UE – União Europeia

UNCTAD – United Nations Conference on Trade and Development (Conferência das Nações Unidas sobre Comércio e Desenvolvimento)

UNHRC – United Nations Human Rights Council (Conselho de Direitos Humanos da ONU)

SUMÁRIO

Apresentação **16**

1. Da razão de Estado à governança algorítmica: condições internas e externas para uma assemblage global da vigilância **28**

1.1 Considerações sobre a segurança como tecnologia de governo 29

1.2 Regimes de visibilidade e mutações tecnopolíticas: do panoptismo à dispersão algorítmica 35

1.3 A política internacional da vigilância: uma gramática em três tempos 50

2. Arquiteturas institucionais da vigilância para uma economia política da privacidade **61**

2.1 Instituições, interpretações e mercados de dados: alguns alicerces do capitalismo da vigilância 62

2.2 Do Estado ao Mercado, o paradigma neoliberal das sociedades da vigilância 74

2.3 Governança, vigilância e algumas anotações sobre o colonialismo de dados 82

3. A privacidade como agenda política **98**

3.1 A emergência histórica da privacidade e da proteção de dados 99

3.2 A governança global da privacidade: instituições, regimes e assimetrias normativas 108

3.3 O caso do GDPR: introduzindo o dispositivo privacidade 121

4. A experiência brasileira da governança de dados: disputas, normativas e governamentalidade **132**

4.1 Antecedentes institucionais e heranças autoritárias 132

4.2. A digitalização do Estado brasileiro e algumas condições de possibilidade para uma Lei Geral de Proteção de Dados 136

4.3 O caso da LGPD: instrumentos e implicações à luz do dispositivo privacidade 141

Considerações Finais **148**

Anexo I **155**

Anexo II **158**

Anexo III **163**

Anexo IV **166**

Anexo V **168**

Anexo VI **171**

Anexo VII **173**

REFERÊNCIAS **177**

Apresentação

Todas as razões para fazer uma revolução estão aí. Não falta nenhuma (...)

- de nada somos poupados, nem mesmo de estar informados sobre isso. (...)

Todas as razões estão reunidas, mas não são as razões que fazem as revoluções, são os corpos.

E os corpos estão diante das telas.

(Comitê Invisível, 2020 - Motim e Destituição Agora, n-1)

Esta tese começa, entre 2020 e 2021, a ser produzida sob circunstâncias incomuns de seu próprio tempo, grande parte delas marcada por dois anos de pandemia no planeta e pelo que sobrou dela, para o bem e para o mal. Tal como tantas outras gestadas sob condições semelhantes, não poderia ser diferente. Tempos de outras espaço-temporalidades, de outras partilhas, de aproximações e distâncias, de outras imaginações, por vezes de imaginação nenhuma diante do colapso sistêmico aparentemente inevitável. Tempos que parecem selar a derrota do Comum e do cuidado, e o império da dissociação e do extermínio. Em particular para aqueles de nós que testemunhamos o arquitetado descontrole da catástrofe político-sanitária no Brasil e suas ramificações *kafkianas,* as mais hediondas prioridades do neoliberalismo pandêmico-colonial-securitário parecem nitidamente estampadas em todo horizonte (in)visível: o extrativismo e a crise climática, o controle e violência de Estado - e sobretudo suas mediações tecno autoritárias.

Para o recorte que nos concerne neste trabalho, a conjuntura é particularmente fortuita na medida em que, sob a cortina de fumaça da "gestão" da pandemia, a discussão a respeito da atualização de protocolos em torno da digitalização da vida social progride como um setor de especial atenção, com a consolidação por exemplo da Doutrina Nacional de Segurança Cibernética e o estabelecimento da tardia Estratégia Nacional de Segurança Cibernética (E-Ciber), o primeiro registro oficial dos princípios brasileiros para o desenvolvimento do setor no futuro imediato. Este marco é acompanhado pela intensa adaptação das atividades mais variadas do cotidiano íntimo e produtivo do país ao mundo virtual, bem como pela

subsequente multiplicação de ameaças que supostamente emergem de vulnerabilidades ditas intrínsecas ao ciberespaço. Ao mesmo tempo, alinhada a tendências planetárias, o Brasil robustece seu aparato de vigilância estatal, legitimado pela percepção acentuada de não-tão-novos riscos, com a adoção de medidas excepcionais de governo das populações - na forma por exemplo de dispositivos de reconhecimento facial e biométrico e coleta irrestrita de dados pessoais por programas de monitoramento computo-informacionais empregados por forças policiais e uma variedade de agências governamentais. Embora a hipótese de que este processo coincide apenas com a recente ascensão de uma figura com ambições autoritárias à presidência da república seja sedutora, uma breve recuperação dos acontecimentos que parecem se reportar ao atual estado das coisas rapidamente sugere outra possibilidade, coerente com a perspectiva de que a democracia contemporânea é aliada imanente da exceção, ponto ao qual voltaremos mais adiante.

A cultura política da vigilância no Brasil, entretanto, tem raízes históricas profundas. Durante a Ditadura Militar (1964–1985), o Serviço Nacional de Informações (SNI) desempenhou papel central na sustentação do aparato repressivo do regime, legitimado pela Doutrina de Segurança Nacional. A noção de "inimigo interno" era suficientemente ampla para abranger qualquer cidadão considerado potencialmente subversivo. A redemocratização e a Constituição de 1988 garantiram o direito à privacidade, mas mantiveram brechas legais que permitiram a interceptação de comunicações, formalmente regulamentada apenas em 1996, no governo Fernando Henrique Cardoso. Tal continuidade evidencia como a transição democrática não eliminou as lógicas de vigilância herdadas do regime autoritário. Na década seguinte, o tema retornou ao centro do debate público com a CPI dos Grampos (2007–2009), que revelou a extensão das interceptações telefônicas no país e a atuação de empresas de tecnologia sem regulação específica. Entre elas, destacou-se a Dígitro, desenvolvedora do sistema Guardião, plataforma de interceptação e análise de voz amplamente utilizada por órgãos de segurança. Estimativas públicas indicavam que, por volta de 2018, o sistema concentrava a maior parte das soluções de inteligência disponíveis no mercado, o que reavivou questionamentos sobre transparência e *accountability*.

O cenário internacional, de igual maneira, influenciou fortemente o debate brasileiro. Em 2013, as revelações de Edward Snowden sobre o programa PRISM da NSA — divulgadas por Glenn Greenwald — expuseram a espionagem de comunicações de líderes estrangeiros, incluindo a então presidenta Dilma Rousseff. A resposta diplomática brasileira,

à época, foi considerada contundente, denunciando as práticas de vigilância global nas Nações Unidas e propondo a criação de marcos regulatórios internacionais para a proteção da privacidade. O episódio impulsionou debates internos sobre soberania digital, segurança cibernética e governança da Internet, resultando na aprovação do Marco Civil da Internet (Lei nº 12.965/2014). A tramitação do Marco Civil consolidou princípios de neutralidade da rede e proteção de dados, mas também reforçou mecanismos de vigilância estatal, como a obrigatoriedade do armazenamento de registros de conexão por provedores de acesso, ilustrando a tensão permanente entre privacidade e segurança no interior do referido debate. O período subsequente, marcado pelas Jornadas de Junho de 2013, pela Copa do Mundo (2014) e pelos Jogos Olímpicos (2016), reforçou essa ambiguidade. Os megaeventos legitimaram a expansão dos Centros Integrados de Comando e Controle, dos sistemas de monitoramento em tempo real e das chamadas rondas virtuais, consolidando o cenário brasileiro como o de um laboratório de tecnologias de vigilância urbana.

Nos anos seguintes, multiplicaram-se iniciativas de segurança digital, na forma por exemplo do Comando de Defesa Cibernética (ComDCiber), vinculado às Forças Armadas, e do reforço das atribuições do Gabinete de Segurança Institucional (GSI) e da Agência Brasileira de Inteligência (ABIN). A Estratégia Nacional de Segurança Cibernética (E-Ciber), lançada em 2020, formalizou esse ecossistema, incorporando elementos da política de defesa e da governança digital sob o argumento da proteção de infraestruturas críticas. Em paralelo, amadurecia o debate sobre proteção de dados pessoais, impulsionado pelo escândalo da Cambridge Analytica (2018) e pela entrada em vigor do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. Nesse contexto, o Brasil promulgou a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), estabelecendo um marco normativo nacional. A criação da Autoridade Nacional de Proteção de Dados (ANPD), em 2019, completou o arranjo institucional, ainda que sob forte influência do Executivo. A nomeação, em 2020, de diretores ligados ao meio militar gerou preocupações sobre autonomia técnica e captura política. Em 2023, com a transformação da ANPD em autarquia vinculada ao Ministério da Justiça e Segurança Pública, reafirmou-se o vínculo entre as agendas de privacidade e segurança, evidenciando o caráter ambivalente da regulação brasileira.

Pouco tempo depois, ainda em 2018, o presidente em exercício Michel Temer, por meio da MP 869/2018 e sob pressão da sociedade civil pela garantia da eficácia da LGPD,

cria a Autoridade Nacional de Proteção de Dados (ANPD), como um órgão público dentro da Presidência da República, vinculada à Casa Civil, convertida em lei alguns meses depois, em 2019. É, entretanto, apenas em 2020, já sob nova gestão, que o Decreto 10.474 define a estrutura organizacional da ANPD e os requisitos para instalação do Conselho Nacional de Proteção de Dados e da Privacidade, pressupondo a participação de representantes do Poder Executivo, da sociedade civil e do setor produtivo, entre outras instituições, a serem escolhidos e nomeados pelo Presidente da República, mediante aprovação do Senado Federal, levantando preocupações sobre a autonomia decisória e técnica da Autoridade.

Em setembro de 2020 finalmente entra em vigor a LGPD e, em 15 de outubro, a Presidência da República, na figura de Jair Bolsonaro, publica os diretores indicados para o Conselho da Autoridade Nacional de Dados, dentre os quais três seriam membros do exército brasileiro, com pouca ou nenhuma experiência no tema da proteção de dados. Na ocasião, a Coalizão Direitos na Rede alertava para o risco de cooptação do órgão para fins de vigilância estatal e repressão política - e, é claro, para o vácuo de supervisão tecnicamente competente para o tratamento de dados no país. No contexto da reestruturação ministerial de 2023, sob mandato de Lula da Silva, a ANPD perde sua vinculação à Casa Civil e assume o papel de autarquia especial vinculada ao Ministério da Justiça e Segurança Pública, sob prerrogativa de autonomia técnica e decisória, formalizando o laço entre o paradigma da privacidade e o da segurança no cenário normativo brasileiro. Na medida em que, em linhas gerais, este processo se intensifica em resposta a circunstâncias elaboradas internamente em termos de sua excepcionalidade, percebe-se a permanência de um legado de narrativas da segurança que parece ser representação quase emblemática da ruptura normativa característica dos estudos críticos de segurança desde os anos 1990.

Na Europa, observa-se um movimento análogo de consolidação de marcos regulatórios durante a última década, em que crises políticas e tecnológicas serviram como catalisadores. A aprovação do Regulamento Geral sobre a Proteção de Dados (GDPR), em 2016, simbolizou resposta imediata ao crescimento das plataformas digitais, como também um esforço de recuperar a soberania normativa diante do domínio extraterritorial das corporações norte-americanas. A partir de então, sucessivas decisões de adequação — como nos casos do Japão (2019), do Reino Unido (2021) e do Uruguai (2022) — projetaram a União Europeia como epicentro de uma gramática de governança que combina a retórica da proteção de direitos fundamentais com a pragmática de assegurar competitividade global. Tal

como no caso brasileiro, os efeitos da vigilância em massa revelados por Edward Snowden em 2013 atuaram como gatilho, fornecendo legitimidade política para a transformação de dispositivos de proteção antes fragmentários em um regime de alcance global. Nos Estados Unidos, o quadro se delineia de forma distinta, ainda que também impulsionado por inflexões críticas. A ausência de uma lei federal de proteção de dados converteu regimes setoriais, como HIPAA e COPPA, em arranjos incompletos que cederam lugar à ascensão de mecanismos híbridos como o *Privacy Shield* e, mais recentemente, o *Data Privacy Framework*, de 2023, este último estabelecido em resposta à decisão *Schrems II* da Corte de Justiça da União Europeia. Nessa configuração, a legitimação do modelo estadunidense passa pela intermediação corporativa: Big Techs, consultorias globais e certificações privadas moldam o conteúdo material das salvaguardas, traduzindo-as em instrumentos de compliance. O episódio da suspensão de serviços ao WikiLeaks, em 2010, exemplifica esse regime de delegação, em que empresas de infraestrutura digital atuam como braços informais do Estado, redefinindo as fronteiras entre regulação pública e autorregulação privada.

Na região da Ásia-Pacífico, por sua vez, a consolidação de regimes como o APEC Cross-Border Privacy Rules (CBPR) ilustra como a integração econômica pôde se sobrepor ao desenho de direitos fundamentais, inspirado em princípios da OCDE, mas operacionalizado por meio de certificações voluntárias, ao passo que legitima práticas de mercado transfronteiriças ao mesmo tempo em que preserva espaços para variações nacionais. Essa arquitetura sugere como alguns desses padrões regulatórios na região se inscrevem no vocabulário da eficiência comercial, em contraste com o enquadramento europeu da privacidade como direito fundamental. Ao lado de iniciativas domésticas, como a lei japonesa de proteção de informações pessoais, revisada em 2020, ou o modelo sul-coreano centrado em autoridades independentes, emerge um mosaico de regimes que, a despeito da fragmentação, converge para legitimar a intensificação da circulação global de dados.

Na América Latina, a consolidação de marcos regulatórios de proteção de dados assumiu feições próprias, marcadas por processos de transição democrática. A criação da *Red Iberoamericana de Protección de Datos (RIPD)*, em 2003, foi um primeiro esforço de articular uma gramática comum entre diferentes países, ainda que com níveis desiguais de institucionalização. México (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010), Colômbia (Ley 1581, 2012), Uruguai (Lei nº 18.331, 2008, com posterior reconhecimento de adequação pela União Europeia em 2012) e Chile (com reformas

em andamento desde 2018) ilustram diferentes trajetórias de consolidação normativa que, embora inspirados em referenciais europeus, também respondem a pressões internas vinculadas ao legado de vigilância política e ao fortalecimento da integração econômica regional.

A partir dos anos 2010, a circulação internacional de dados passou a ocupar o centro das disputas regulatórias na região. De um lado, a União Europeia promoveu um processo ativo de exportação normativa, estimulando reformas nacionais alinhadas ao GDPR e conferindo selos de adequação como forma de inserção em mercados globais. De outro, práticas de *forum shopping* regulatório evidenciaram a tensão entre regimes mais protetivos, como o uruguaio, e modelos ainda frágeis, como o brasileiro antes da LGPD ou o chileno, até hoje em revisão. Esse cenário foi atravessado por episódios que expuseram a vulnerabilidade regional, como os vazamentos massivos de dados de eleitores no México (2016) ou as denúncias de cooperação tecnológica entre empresas de segurança e governos autoritários. Nesses cenários, a convergência discursiva em torno da proteção de dados como direito humano convive com a terceirização de serviços e dependência tecnológica em relação a potências extrarregionais. Ao espelhar o caso brasileiro, esse panorama evidencia que a institucionalização de autoridades de dados e a formalização de direitos se articulam tanto com a legitimação de práticas de mercado quanto com a atualização de dispositivos securitários — um movimento que conecta a região às tendências globais e, ao mesmo tempo, revela suas assimetrias estruturais. Esses processos, de nossa perspectiva, refletem um padrão mais amplo, segundo o qual crises tecnopolíticas operam como catalisadores da normatização da vigilância, tanto no Brasil quanto no cenário global. A privacidade, nesse contexto, deixa de ser um direito ameaçado e passa a funcionar como dispositivo de governo: um instrumento que organiza condutas, produz subjetividades e delimita fronteiras do aceitável. Esta tese parte dessa hipótese — de que a privacidade, mais do que uma categoria em crise, é um campo de disputa, conforme trataremos no desenrolar de nossos capítulos.

A partir das experiências introdutórias acima descritas, sugerimos que a governança dos dados se inscreve nas Relações Internacionais contemporâneas como expressão de longas continuidades nos modos de organizar o poder global, agora atravessado pela centralidade da informação como recurso estratégico. Ao invés de inaugurar um campo inteiramente novo, a administração dos fluxos digitais reatualiza práticas de controle e hierarquização — historicamente estruturadas pelo comércio, pela finança ou pela guerra — em torno da lógica

contemporânea da exploração, coleta e circulação de dados. A economia política do capitalismo da vigilância oferece, assim, não apenas uma gramática para compreender a mercantilização da vida informacional, mas também um horizonte a partir do qual se articulam novas formas de dependência, legitimação e intervenção no plano internacional. Nessa chave, a governança dos dados não é mero detalhe técnico, mas uma das arenas centrais em que se decide o desenho das assimetrias políticas e econômicas presentes.

As discussões sobre governança da Internet, ainda que frequentemente enquadradas em torno de regimes e instituições, carregam uma ambiguidade conceitual incontornável. A terminologia corrente revela como diferentes atores atribuem sentidos específicos ao digital: enquanto expressões como "ciber" são mobilizadas sobretudo para demarcar o campo da segurança e do combate a crimes, termos como "Internet" ou "digital" aparecem ligados à economia de dados, ao comércio eletrônico ou mesmo às inovações da chamada Internet das Coisas. Essa polissemia não é neutra, pois orienta prioridades políticas e institucionais distintas, legitimando arranjos específicos de regulação e cooperação (DeNardis, 2020; Kurbalija, 2016). A ênfase em "ciber" ganha destaque em determinados contextos geopolíticos, como no caso chinês, em que a narrativa de segurança é convertida em eixo estruturante das políticas digitais e das formas de cooperação internacional. Já em outras arenas, prevalece o uso de "digital" como categoria vinculada a desenvolvimento econômico e inovação, ou de "virtual" para designar ativos emergentes, como criptomoedas. Mais do que diferenças terminológicas, o que se observa é a disputa por enquadramentos normativos que, ao mesmo tempo, orientam o fluxo de investimentos e modulam as expectativas sobre vulnerabilidade e risco. Esse panorama ajuda a compreender por que a segurança aparece como vetor de convergência mais forte, sob o argumento de que não apenas a economia globalizada, mas também a estabilidade política e institucional dependem da integridade das infraestruturas digitais. Contudo, quando o debate se desloca para privacidade, criptografia ou mercados de dados, as divergências se tornam mais visíveis, refletindo tanto particularidades nacionais quanto interesses de corporações transnacionais.

O ciberespaço, além de povoado pelos riscos atribuídos a suas características técnicas intrinsecamente vulneráveis, acompanha inevitavelmente um conjunto de discursos próprios da chamada "Era da Informação". Processos de desterritorialização, compressão espaço-temporal, consolidação das sociedades em rede, reconfiguração do poder do Estado e da impermeabilidade de fronteiras nacionais e ascensão de novos atores e novos saberes

técnicos e especializados são alguns dos elementos comuns no vocabulário de perspectivas ora otimistas, ora pessimistas da virada cibernética (Santos, 2011), que encontram terreno fértil junto às narrativas dos riscos crescentes da (des)ordem internacional que sucedem o fim da União Soviética: no lugar de um grande inimigo no qual convergiam as preocupações do capitalismo ocidental, constata-se uma multiplicidade de potenciais inimigos, interconectados e transversais que demandam, por sua vez, um esforço civilizatório na forma da globalização da lógica da segurança como um bem comum global (Bigo, 2016). Bigo resume:

> A imagem da inimizade certamente continuava a ser central, mas sua definição podia ser difusa e mudar muito rapidamente ao longo do tempo. A incerteza da análise foi transferida para a própria visão de mundo, e o mundo tornou-se, portanto, caótico em si mesmo; a incerteza converteu-se em uma qualidade da estratégia, deslocando-se para um perfil de gestão de riscos. Ao mesmo tempo, a individualização da vida — para sustentar o argumento da proteção de "cada" indivíduo (de um lado) — foi colocada sob o rótulo de um "humanitarismo" da segurança, no qual a humanidade como coletividade global e a humanidade como cada indivíduo isolado estavam interligadas, relativizando a centralidade da segurança nacional (estatal). O policiamento internacional por meios militares, no entanto, continuava a ser uma ação de policiamento, não uma guerra. (...) A segurança externa se volta para a segurança interna. Foi necessária uma nova série de regimes de justificação para reconstruir a segurança externa como desdobramento lógico da segurança interna — como a continuidade do mesmo fenômeno além-fronteiras. A separação foi esquecida, o interestatal desapareceu, mas o global — entendido como uma lógica interna expandida, na qual a sociedade e a sociedade mundial se sincronizam — tornou-se central. (BIGO, 2016, p. 8. Tradução nossa.)

O autor, entretanto, sublinha o caráter político e, por vezes, conservador do argumento em torno do alerta à desordem e a insegurança que, em última instância, aludiria ao imperativo da subordinação *"da justiça criminal a uma lógica preventiva dirigida por serviços de inteligência e suas técnicas intrusivas"* (Bigo, 2016, p. 12. Tradução nossa.). Ao contrário, caberia aí um esforço crítico com enfoque na maneira pela qual a (in)segurança é entendida e vivida, tendo como pano de fundo da análise os objetos aos quais é dirigida tal como suas condições de reprodução. Bigo ainda chama atenção para a centralidade dos serviços de inteligência e das tecnologias de vigilância em um processo de reconfiguração das práticas e políticas de (in)segurança, tal como dos saberes mobilizados em seu entorno (Bigo, 2016, p. 3), e sublinha que abordagens teórico-metodológicas incapazes de se desprender das gramáticas disciplinares, seja da criminologia ou das Relações Internacionais do pós-Guerra Fria, poderiam não identificar a forma pela qual a lógica da segurança contribuiria com a reformulação e limitação de concepções como liberdade, justiça, igualdade e democracia:

> (...) grande parte da discussão na teoria jurídica tem sido formulada em torno da relação entre segurança e proteção de dados-privacidade, ou entre segurança e casos de tortura, bem como das mais graves violações de direitos humanos — mas pouco se discute sobre todos os gradientes nos quais a segurança, longe de equilibrar a liberdade em busca de um novo ponto de estabilidade diante do perigo, está reformulando a própria noção de liberdade, fragmentando seus significados e vestindo-se com algumas de suas roupagens. (BIGO, 2016, p.13. Tradução nossa.)

Diante do exposto, a presente reflexão buscará compreender a lógica de uma possível gramática da privacidade na configuração de arcabouços normativos multilaterais de "boas práticas" de governança e proteção de dados em um panorama internacional marcado por uma racionalidade neoliberal de subjetividade securitária. Pressupondo a (in)segurança como um projeto atravessado por uma governamentalidade orientada pelo autogoverno do indivíduo enquanto capital humano e pela produção de uma subjetividade securitária (AUGUSTO e WILKE, 2019), procuramos também verificar em que medida se torna possível falar em termos de um *dispositivo privacidade* coerente com a reprodução de um estado de monitoramento infinito, regulação e intervenção característico da democracia contemporânea (PASSETTI et al., 2019).

Por *dispositivo*, lembramos, Michel Foucault se refere mais do que ao "*conjunto heterogêneo que engloba discursos, instituições, organizações arquitetônicas, decisões regulamentares, leis, medidas administrativas (...)"* (FOUCAULT, 2000, p. 244.), mas a uma formação *"que, em um determinado momento histórico,* ***teve como função principal responder a uma urgência.*** *O dispositivo tem, portanto, uma função estratégica dominante*" (FOUCAULT, 2000, p. 244, grifo nosso). Trata-se, portanto, de uma composição fundamentalmente heterogênea de elementos sem nítida distinção (DELEUZE, 1992, p. 160) que distribuem o visível e o invisível, produzindo determinados "regimes de enunciação" (DELEUZE, 1992, p. 160) correspondentes a determinadas configurações históricas. Em sua dimensão estratégica, que aqui nos concerne profundamente, veremos que o *dispositivo* pressupõe um "duplo processo" (FOUCAULT, 1979, p. 245) de concepção e administração da crise, da qual ele mesmo é efeito e instrumento.

Considerando a perspectiva das Relações Internacionais, a escolha pelo conceito é particularmente pertinente, na medida em que problematiza a perspectiva de um aparato estatal não limitado a seus componentes institucionais; pelo contrário: "*ao invés de tomar as instituições como ponto de partida, ela foca nas tecnologias que são materializadas e*

estabilizadas em configurações institucionais" (LEMKE, 2018, p. 44). Como veremos, na forma de processos de direção da vida, o *dispositivo* articulará, uns sobre os outros, objetos, sujeitos, elementos discursivos e não discursivos, relações de comunicação e de poder, pressupondo sobretudo uma analítica de governo ancorada na identificação de *"alguma força problemática e de agência (...) carente de ser formada, configurada e dirigida"* (LEMKE, 2018, p. 48). Como "máquinas criadoras de mundos" (LEMKE, 2018) o *dispositivo* se materializa e reconfigura através do tempo e do espaço de maneira incontornavelmente dinâmica.

Nesse sentido, emprestaremos a contribuição do autor também no que diz respeito à genealogia como método analítico histórico-político (BONDITTI et al., 2015), pressupondo consequentemente a segurança cibernética no referido contexto não como um fenômeno acabado, mas buscando analisá-la, de fato, em termos dos saberes e tecnologias políticas mobilizadas seu processo de constituição. Procuramos, sobretudo, investigar a maneira pela qual a expressão supracitada costurou, efetivamente, a produção normativa em torno da "gestão" da ameaça cibernética em perspectiva genealógica, ou seja, de forma a *"intervir no presente, identificando discursos (políticos, econômicos, jurídicos e sociais) vitoriosos em um determinado momento"* (MAIONE e RODRIGUES, 2019, p. 155). Relembramos, assim, que

> (...) a genealogia se foca não em "objetos" rígidos e supostamente isoláveis do conjunto dos acontecimentos sociais. Voltadas às controvérsias ao redor da definição e construção dos diversos "objetos", a genealogia interpela os acontecimentos, discursos e práticas de poder interessados em identificar quais relações de poder e saber moldaram esse objeto. Como uma determinada questão, uma determinada causa ou objetivo político é produzido enquanto "problema", ou seja, enquanto um tema a ser equacionado, teorizado, classificado e regido por um conjunto específico de normas e práticas de governo (MAIONE e RODRIGUES, 2019, p. 156)

Consideramos também significativo o esforço de adotar como pano de fundo, ao mesmo tempo, a contribuição de Donna Haraway quanto à noção de *saberes situados* (HARAWAY, 1988) - que pretende problematizar tanto o universalismo quanto o relativismo absoluto - e a compreensão de epistemologias *dataficadas* (COULDRY e MEJIAS, 2019) como uma articulação sociotécnica contemporânea da colonialidade do poder (RICAURTE, 2019), conforme Ricaurte:

> Este modelo explica como a colonialidade do poder se materializa como um conjunto de processos que determinam a coleta, o armazenamento, o acesso, a análise e o uso de dados (...) enfatiza a centralidade dos dados e dos

> algoritmos, bem como as infraestruturas materiais e simbólicas, tecnologias, modelos de negócios emergentes, atores e práticas que cercam a coleta, o armazenamento/acesso, a análise e o uso de dados. Contextualiza o colonialismo de dados em um arranjo de processos que fazem parte de uma epistemologia dominante que se traduz na dominação de corpos, afetos e territórios. (RICAURTE, 2019, p. 356. Tradução nossa)

Concordamos, diante disso, com a antítese de Yuk Hui contrária ao universalismo tecno determinista, segundo a qual os artefatos encontrariam limites e possibilidades de funcionamento diversas diante de cosmologias particulares, para além da funcionalidade e da eficiência (HUI, p. 25). Mais do que isso, compreendemos que a conjuntura recente traz indícios da emergência para se repensar a questão da tecnologia na aproximação do chamado Antropoceno, como anunciado por Hui, permitindo - com esforço - avistar um horizonte tecnológico de cosmotécnicas autônomas, em face de novos (ou renovados?) dispositivos de dominação. De que maneira a construção da privacidade como um objeto a ser assegurado, no interior de formulações típicas de epistemologias dataficadas, implica em um processo de subjetivação coerente com sujeitos traduzidos em termos de gestores de risco? E quais as implicações dessa construção no contexto de um Brasil marcado pelas expressões da hipótese da colonialidade do (ciber)poder? São algumas das questões às quais a presente tese se reportará.

À luz do exposto, entende-se que esta reflexão se situa em uma intersecção transdisciplinar por excelência, na medida em que evoca o campo dos chamados estudos da vigilância (MONAHAN e WOOD, 2018), marcadamente caracterizado pelos (des)encontros teórico conceituais com uma variedade de campos do saber - dentre os quais as Relações Internacionais permanecem sub representadas, inclusive. Buscaremos, nesse sentido, recuperar o arcabouço da área de maneira a agregar à análise das referidas práticas de governança internacional, a fim de caracterizar a maneira pela qual a literatura da vigilância elucida os padrões de observação, regulação e modulação comportamental em torno, por vezes, da pressuposição oculta da privacidade como uma resposta normativa a ser perseguida. Para tanto, organizaremos nossa reflexão em quatro capítulos. O primeiro deles busca reconstruir do ponto de vista teórico e conceitual a perspectiva de que a sociedade contemporânea corresponde a uma atravessada por práticas difusas e descentralizadas de monitoramento permanente e, em um segundo momento, compreender de que forma essa perspectiva foi traduzida em termos da percepção da comunidade internacional em torno de episódios de vigilância massiva. O segundo capítulo procurará identificar de que maneira o

contexto genericamente descrito seção anterior poderá ser compreendido de forma mais detalhada em termos de seu delineamento na forma de uma arquitetura institucional - política e produtiva - compatível com o que chamaremos de economia política da privacidade (que responderá, inevitavelmente, a uma economia política da vigilância). No capítulo 3, finalmente, nos debruçaremos sobre a emergência histórica da noção moderna de privacidade para, então, compreender de que forma o cenário desenhado nos capítulos 1 e 2 contribuirá para ressignificar uma agenda política da proteção de dados no século XXI, na qual localizaremos nossa hipótese do *dispositivo privacidade*. O capítulo 4, por fim, olhará com mais atenção para a experiência brasileira, brevemente descrita nesta apresentação, procurando situar a reflexão do capítulo 3 em uma conjuntura marcada sobretudo pela condição do colonialismo de dados.

1. Da razão de Estado à governança algorítmica: condições internas e externas para uma *assemblage* global da vigilância

Partimos do pressuposto de que práticas e políticas de monitoramento e vigilância, longe de se restringirem a coleta passiva de informações, devem ser compreendidas como uma tecnologia política profundamente enraizada na formação dos modos modernos de governar. Este capítulo assume a noção foucaultiana de segurança como tecnologia de governo, para explorar como a vigilância opera como dispositivo central na administração dos riscos, na produção de sujeitos e na gestão da vida. Recapitulando a transição da soberania para a segurança como tecnologia de governo primordial, exploramos a emergência do panoptismo como racionalidade disciplinar e seus desdobramentos em formas cada vez mais descentralizadas, capilares e integradas aos fluxos de informação, característicos do que chamaremos, mais adiante, de virada cibernética. A vigilância, portanto, será aqui entendida como um regime de visibilidade e ordem (WOOD, 2016), produtora de efeitos de controle e normalização por meio da organização estratégica dos olhares.

O capítulo está dividido em três seções. A primeira pretende examinar a vigilância no interior das tecnologias modernas de governo, explorando seus desdobramentos no processo de governamentalização do Estado. Em um segundo momento, traçaremos uma breve recuperação da noção da vigilância moderna, do modelo panóptico às formas atuais de monitoramento distribuído e algorítmico, articulando a visibilidade como um operador crucial da ordem contemporânea. Na terceira seção discutiremos algumas das mobilizações da problemática da vigilância no campo das relações internacionais para, por fim, prepararmos o terreno para nosso segundo capítulo, no qual procuraremos efetivamente articular esse cenário com racionalidades e os desafios impostos pela governança global da privacidade.

A partir da analítica foucaultiana da segurança como tecnologia de governo, pretendemos aqui recuperar os deslocamentos históricos que moldaram a racionalidade governamental contemporânea, a partir da percepção de que a segurança emerge como um mecanismo que não elimina o risco, mas o administra, regulando fluxos populacionais, corpos e condutas. Tendo essa reflexão como ponto de partida, elaboramos aqui uma reconstrução das procedências das práticas de vigilância contemporâneas não como exceção autoritária, tampouco como retorno ao regime disciplinar, mas como dispositivo técnico-político que se inscreve de forma particular nos circuitos da normatividade cotidiana em sua constituição

atual. Ao mesmo tempo, esperamos introduzir a suposta oposição entre segurança e privacidade como uma falsa dicotomia, historicamente determinada e pertinente a determinadas racionalidades de governo, conforme trataremos no Capítulo 2. Para tanto, compreendemos a "segurança" enquanto categoria fundacional da modernidade ocidental sobretudo enraizada na administração da vida social, marcada pela transição típica do século XVIII, conforme elaborada por Michel Foucault em *Segurança, Território, População* (2008). Assumindo a regulação dos riscos como tarefa privilegiada, a segurança moderna pressupõe entidades dotadas de comportamentos previsíveis e sujeitas a intervenções administrativas, por exemplo, da estatística, da medicina social e do planejamento urbano. Trata-se, como abordaremos mais adiante - para Foucault - de uma tecnologia de governo traduzida em termos de "possibilitar, garantir e assegurar a circulação" (FOUCAULT, 2008, p. 29. Tradução e grifo nossos.) - uma que será posteriormente atravessada pela adesão de tecnologias computo-informacionais e reconfigurada na forma contemporânea sobre a qual nos debruçaremos mais adiante.

1.1 Considerações sobre a segurança como tecnologia de governo

A genealogia do poder em Michel Foucault revela uma transformação profunda na forma como os indivíduos e as populações são administrados a partir do início da chamada modernidade. Não necessariamente na forma da substituição das tecnologias de poder ou por sua sucessão linear, mas pela emergência de diferentes racionalidades de governo que passam a se sobrepor: o poder soberano, centrado no direito de matar ou deixar viver, o poder disciplinar, que individualiza e normatiza os corpos, e, por fim, a biopolítica, alicerce de uma nova tecnologia de governo voltada para a gestão da população pela intervenção da segurança (FOUCAULT, 2008a; FOUCAULT, 2008b).

Marcada por uma lógica jurídico-repressiva, a soberania, para Foucault, tem como princípio fundante a centralização do poder na figura do soberano que guarda a prerrogativa de intervenção sobre um determinado território e seus súditos. Típico do Antigo Regime, o poder soberano opera por meio de leis proibitivas e punições violentas (FOUCAULT, 2005). Nas chamadas sociedades disciplinares, por sua vez, respondendo às demandas do capitalismo industrial, o autor identifica práticas de vigilância modeladas à luz do emblema do panóptico de Bentham, operando por meio da exclusão e da censura e produzindo corpos dóceis e previsíveis, em substituição das práticas punitivas do poder soberano. No contexto da

predominância do panoptismo, o poder disciplinar se projeta inicialmente sobre os indivíduos e, progressivamente, sobre toda uma coletividade conduzida a um modelo de normalização sustentado por uma lógica "negativa". Nesse horizonte, não há espaço para aqueles que escapem da norma estabelecida como aceitável, nem para que os sujeitos mantenham, em seu interior, zonas de opacidade ou resistência que fujam ao regime normativo.

Com a expansão das técnicas de governo próprias das monarquias administrativas, entretanto, instala-se uma nova racionalidade, que nosso autor chamará de governamentalidade (FOUCAULT, 2008a). O conceito articula três elementos: o surgimento de uma série de instituições, saberes e dispositivos voltados à condução da conduta dos indivíduos e das populações; o deslocamento do poder jurídico-repressivo para uma racionalidade de governo baseada na otimização das forças sociais e econômicas; e a constituição do Estado moderno como efeito e condensação desse novo conjunto de práticas governamentais emergentes. Diferentemente do observado no contexto do paradigma disciplinar, a governamentalidade moderna passa a se organizar efetivamente em torno da pergunta: como governar a vida em sua multiplicidade e imprevisibilidade constitutiva (FOUCAULT, 2008b)?

Contrastando com o modelo disciplinar (FOUCAULT, 2008a), é nesse contexto que emerge a segurança como tecnologia de governo implicando em uma inflexão-chave: enquanto a disciplina buscava moldar comportamentos a partir da norma e da vigilância contínua, o novo modelo não visa eliminar o risco, mas governar o acaso. A partir do século XVIII, portanto, novas formas de gestão passam a adotar o aleatório como parte constitutiva do real: os acidentes, as epidemias, os fluxos econômicos, os movimentos populacionais, Desloca-se a segurança para o centro da intervenção, seja por meio da previsão, da normalização e da regulação de comportamentos em grande escala, mobilizando instrumentos como o censo, a demografia, a análise dos preços e dos mercados (FOUCAULT, 2008a FOUCAULT, 2008a). Uma nova racionalidade fundamentalmente biopolítica - ou seja, no governo da vida das populações (FOUCAULT, 2008a).

Se, por um lado, a disciplina havia atuado sobre os corpos individuais e a soberania em torno das leis e nos territórios, a segurança se inscreve em um espaço aberto e probabilístico. Em vez de corrigir os desvios, buscará permiti-los dentro de limites aceitáveis, redefinindo o normal na forma do estatisticamente previsível (FOUCAULT, 2008a). Nesse

sentido, a segurança introduz uma lógica de otimização das condições possíveis e desejáveis, sendo, portanto, inseparável das transformações do capitalismo de sua época (FOUCAULT, 2008b. FOUCAULT, 1999), configurando-se como a técnica do governo liberal por excelência: um governo que se auto restringe, que se limita para potencializar os mecanismos do mercado, mas que, ao mesmo tempo, produz as condições para que esses mecanismos sejam eficazes, sobretudo por meio da produção de sujeitos responsáveis, da liberdade calculada e da normatividade difusa (FOUCAULT, 2008b). Deslocando o centro do governo para o futuro incerto, a segurança adota o risco, a probabilidade e a prevenção como seus parâmetros de operação, tornando-se a tecnologia privilegiada de um governo que não apenas reprime ou disciplina, mas que incita, organiza, regula e gera condutas sob a lógica da racionalidade econômica e da gestão do risco.

À luz da nova razão econômica, de inspiração fisiocrata, o Estado reorienta seu objeto primordial de governo a partir daqueles processos e detalhes concebidos como de ordem "natural", ou inevitável, todavia sem necessariamente procurar interrompê-los ou preveni-los - Pelo contrário, trata-se de "deixá-los ser". Nesse sentido, aliada à essa nova racionalidade governamental, insurge a forma de liberdade intimamente aliada à produção da segurança:

> Um aparato de segurança (...) só pode operar adequadamente sob a condição de que lhe seja concedida a liberdade, no sentido moderno adquirido no século XVIII: não mais as isenções e privilégios ligados a uma pessoa, mas a possibilidade de movimento, de mudança de lugar e de processos de circulação tanto de pessoas quanto de coisas. Penso que é essa liberdade de circulação, no sentido amplo do termo — é em termos dessa opção pela circulação — que devemos compreender a palavra liberdade, entendendo-a como uma das facetas, aspectos ou dimensões do funcionamento dos aparatos de segurança. (FOUCAULT, 2008a, p. 49. Tradução nossa.)

É precisamente no interior da incerteza sobre a totalidade dos processos e do futuro, característica do *homo economicus* do liberalismo, que se situa a conciliação entre a liberdade e a segurança (AMOORE, 2013, p. 7), conciliação que opera como a resposta de sua época a permanente problemática do encontro entre a economia e o Estado (a mesma problemática que, em essência, corresponde para Foucault ao próprio cerne da "arte de governar"). É na figura da *população*, emergente neste contexto, que a soberania se desloca da autoridade estritamente jurídica para uma que, cada vez mais, adotará saberes econômicos para governar a conduta de sujeitos econômicos, motivados pela perseguição de seus próprios interesses -

incompatíveis, em certa medida, com a figura totalizante do soberano do século XVII. Foucault resume:

> (...) para que a governamentalidade possa conservar seu caráter global sobre o conjunto do espaço de soberania, para que ela não tenha tampouco que se submeter a uma razão científica e econômica (...), é preciso dar à arte de governar uma referência, um espaço de referência, um campo de referência, uma realidade nova sobre a qual se exercerá, e esse campo novo é, creio eu, a sociedade civil (FOUCAULT, 2008b, p. 400)

Representando, nesse sentido, o solo privilegiado para a consolidação de uma política da vida - ou, biopolítica -, regulada pela lógica da circulação, o liberalismo moderno efetivamente redefine o escopo da prática governamental, na direção de representações ainda mais difusas e modulares do exercício do poder. Na forma do regime que, de fato, fabricará a liberdade (da circulação) (FOUCAULT, 2008b, p. 95) é o liberalismo que fabricará também a gama de limitações e riscos que virão em sua decorrência, implicando em última instância na reprodução perpétua da percepção, ou da realidade, do perigo - esteja ele no presente, no passado ou no futuro -, dos *"perigos cotidianos, perpetuamente animados, atualizados, postos em circulação (...)"* (FOUCAULT, 2008b, p. 97). Não haveria, portanto, *"liberalismo sem a cultura do medo"* (FOUCAULT, 2008b, p. 97).

Em consequência desse processo, "a arte liberal de governar" implica no crescimento vertiginoso de contrapartidas e contrapesos à permanente fabricação da liberdade, seja na forma de controle e intervenção pela vigilância constante ou, contra-intuitivamente, na forma de mais liberdade, esta por sua vez introduzida por mais controle e intervenção: *"temos (...) processos de obstrução que fazem com que os mecanismos produtores de liberdade, os mesmos convocados para assegurar e fabricar essa liberdade, tenha de fato efeitos destruidores que suplantam aquilo que produzem."* (FOUCAULT, 2008b, p.101). Pela fabricação da liberdade, portanto, o governo liberal cultivará *o risco* a ser objeto permanente da segurança. É, portanto, no Estado *governamentalizado* que se consolidará a percepção e construção do risco a ingerência do dispositivo de segurança, cuja operação sobre um território se dará por meio de um conjunto de técnicas, de relações e de domínios, pretendendo responder a um futuro que não é, de fato, mensurável ou inteiramente controlável, mas sujeito a estimativas de probabilidade (FOUCAULT, 2008b, p. 27).

Contemporaneamente, a noção de risco corresponde a uma operadora fundamental do encontro entre a segurança e a vigilância (BRUNO, 2013). De maneira geral pensada em

termos da probabilidade futura da ocorrência de um evento, considerando ações que se dão no presente, para Fernanda Bruno (2013) a lógica do risco implica no *"controle do indivíduo através da responsabilidade"* (BRUNO, 2013, p. 38):

> A identificação do risco é simultânea à identificação dos elementos que aumentam ou diminuem a sua probabilidade de ocorrência, elementos esses que dependem de decisões e ações humanas. Por exemplo, ao se identificar o risco de se desenvolver uma certa doença no futuro, identifica-se num mesmo movimento as ações (dietas, medicamentos, atividade física etc.) que poderiam evitar o aparecimento desta doença, atrelando assim o futuro e o sofrimento a decisões tomadas no presente. Entretanto, o fato de a lógica do risco tornar os indivíduos ou qualquer agente coletivo – como empresas, instituições, governos etc. – **responsável pelos sofrimentos futuros que lhes são anunciados não confere a eles o controle pleno deste futuro**. Evidentemente, tanto o sofrimento antecipado quanto a sua capacidade em evitá-lo são apenas prováveis, e não necessários. Ainda que se faça tudo para evitar o sofrimento em questão, ele pode advir. Do mesmo modo, pode não ocorrer, ainda que nada se faça. (BRUNO, 2013, p. 38. Grifo nosso.)

É na crise do Estado de bem estar social, nos anos 1980, que é possível localizar a transição do "risco" como uma terminologia própria da economia para uma perspectiva hegemônica (BRUNO, 2013; ERICSON e HAGGERTY, 1993) dos problemas disponíveis no horizonte da vida social. Alinhada a formas liberais de governo, a gestão de risco como articuladora do dispositivo de segurança produz identidades coletivas (ERICSON e HAGGERTY, 1993), se configurando em termos de uma "aritmética política" modulando os destinos das populações. É essa reflexividade, em certo sentido, que marcará o governo liberal, na forma de mecanismos de vigilância que se voltam para o próprio governo, permitindo a emergência de reivindicações e contestação social, em clara oposição ao paradigma disciplinar. O liberalismo e o risco, nesse sentido, se articulam de forma indissociável (ERICSON e HAGGERTY, 1993; BARRY et al., 1996), na medida em que possibilitam de forma combinada a institucionalização da vigilância difusa e permanente (WOOD, 2016) Embora não elimine os demais mecanismos de poder, Foucault identifica a governamentalidade liberal como uma que tenderá a predominar sobre os demais, agregando tecnologias de poder em torno do controle das condutas, potencializadas na forma da emergência de um Estado altamente burocrático.

Gandy (1993) identifica, em direção semelhante, a inscrição do sujeito liberal em arquivos digitais legíveis por máquinas, na forma de credenciais pessoais e dados financeiros, educação, emprego, consumo, seguros e registros legais - todos setores moldados, no referido contexto, por processos de vigilância altamente burocratizados, incluindo coleta e armazenamento de informações, monitoramento de indivíduos, estímulo à autogestão, instruções normativas, organização de espaços físicos e supervisão da conformidade com padrões de risco. A capacidade de implementar e sustentar esses mecanismos aparece como determinada pelos recursos disponíveis, pela centralização e acessibilidade da informação, a articulação em rede com outras burocracias, inovação institucional, conformidade legal e, acima de tudo, pela aceitação das populações de que tais mecanismos lhe trariam benefícios, permitindo-lhes governar a si mesmas. O autor detalha, ainda, três processos contínuos que constituem as práticas de vigilância liberal: identificação de perigos, classificação de riscos e avaliação, todas responsáveis pela determinação conjunta de padrões de risco aceitáveis e pela distribuição de vulnerabilidades de acordo com determinadas categorias populacionais.

Com o desenvolvimento de tecnologias de comunicação e informação, a literatura procurará enfatizar a transcendência das práticas de vigilância do controle humano direto. Nesse contexto, a vigilância viabiliza o exercício do poder estatal sem contato direto com os governados, utilizando estatísticas probabilísticas e tecnologias de sensoriamento remoto para permanecer categorizando populações segundo critérios da lógica do risco. A metáfora do *panoptic sort*, de Oscar Gandy (1993) ilustra essa transformação, propondo a existência de um panóptico expandido, organizando toda a vida social em uma máquina hierárquica de classificação e exclusão, modulando comportamentos conforme valores institucionais e acesso a espaços de conhecimento.

Nos debruçaremos sobre a renovação ou o abandono da referência ao paradigma disciplinar na sessão seguinte, considerando para tanto que é ao localizar a gramática do risco como uma das principais legitimadoras dos aparatos de vigilância atualizados para o governo da segurança, Bruno (2013) sediará um terreno propício para a combinação complexa de permanências e rupturas entre as sociedades disciplinares e as sociedades de controle (DELEUZE, 2000). Enfatizamos, portanto, que o processo que recuperamos não implicou em descartar o panoptismo, mas em inseri-lo em conjugações híbridas entre soberania, segurança e disciplina, em um contexto de deslocamento da ênfase da visibilidade e do controle para a gestão contínua de riscos difusos, antecipando debates atuais sobre governança algorítmica e

capitalismo de vigilância, que veremos no capítulo 2. É diante desse cenário que, então, nos voltaremos à atualização das referidas práticas, em termos de regimes de visibilidade contemporâneos, e suas especificidades em relação aos marcos da segurança e da vigilância modernas.

1.2 Regimes de visibilidade e mutações tecnopolíticas: do panoptismo à dispersão algorítmica

Em linhas gerais, o que se convencionou chamar de práticas de vigilância tem se relacionado a técnicas de observação regular e sistemática e intervenção em indivíduos ou populações (Bruno, 2013) a partir de modalidades variadas - analógicas, digitais, mecânicas, eletrônicas - e a serviço de uma série de funcionalidades, em geral situadas no interior da noção da "condução de condutas" de Michel Foucault (2004).

Já amplamente teorizada em termos de sua concepção moderna, a vigilância é, também, frequentemente associada à burocratização da administração do Estado e à expansão de empreendimentos econômicos ao longo do século XIX (LYON, 2013). Desde a contribuição clássica de Anthony Giddens (1987) e Christopher Dandeker (1990), *vigiar* estaria no pódio substancial das instituições modernas, junto da industrialização, do desenvolvimento capitalista e da profissionalização militar, todas instâncias caracterizadas por complexos organizacionais e administrativos profundamente marcados pela produção e armazenamento de dossiers individuais para fins de coordenar e controlar condutas de seus membros, unidades ou funcionários. Já no século XX, no pós-Segunda Guerra, observa-se a expansão dos sistemas modernos de observação, coleta e armazenamento de informações na medida em que o Norte Global se via em transição para modelos de Estados de bem-estar social, acompanhados de uma nova tendência da vigilância em função da cidadania e da participação social (LYON, 2013):

> O Estado liberal facilitou o capitalismo por meio das leis de propriedade e de contrato, além de estabelecer mecanismos de controle sobre a moeda e os monopólios. Contudo, em meados do século XX, o capitalismo passou a manter uma relação mais estreita com o Estado, o que, por um período, reduziu as forças de mercado devido à intervenção da administração burocrática. Esse processo impulsionou o crescimento das práticas de vigilância, especialmente dentro das grandes empresas. Já na década de 1980, contudo, tornou-se evidente que uma nova transformação estava em curso, concebida de diferentes maneiras como "reestruturação" ou "capitalismo desorganizado". (LYON, 2013, p. 36. Tradução nossa.)

Por óbvio, o contexto ao qual Lyon se refere acima - da gradual inflexão para a década de oitenta - é profundamente determinado pela aceleração da circulação possibilitada pela difusão e popularização de tecnologias de comunicação e informação características da virada cibernética (SANTOS, 2003). Período de acelerada "*difusão do capitalismo em escala mundial, permitindo ao capital acessar a dimensão informacional da realidade e submetê-la a um processo de valorização capaz de explorar as suas virtualidades"* (MARIUTTI, 2020, p. 1), a virada cibernética, conceito mobilizado por Laymert Garcia dos Santos (2003), recorda a especificidade da cibernética enquanto uma síntese inovadora que, ao final da década de sessenta, elevou a informação para o centro da "natureza" (MARTINS, 2000) social. A "aceleração da aceleração" (SANTOS, 2003) do desenvolvimento tecnológico e da ampla informatização da sociedade implicou, nesse sentido, na transformação profunda dos saberes. Laymert resume:

> A informação enquanto diferença que faz a diferença reconfigura o trabalho, o conhecimento e a vida, enquanto a virada cibernética transforma o mundo num inesgotável banco de dados. Em toda parte, e sempre que possível, o capitalismo de ponta passa a interessar se mais pelo controle dos processos do que dos produtos, mais pelas potências, virtualidades e performances do que pelas coisas mesmas. O capital, e antes de tudo o capital financeiro, começa a deslocar-se para o campo do virtual, voltando-se para uma economia futura cujo comportamento é analisado por meio de simulações cada vez mais complexas. Tal tendência não se limita porém ao mercado financeiro; em muitos outros setores a prospecção passa a preponderar. (...) **É possível compreender todo esse deslocamento por meio da importância ascendente da informação, tal como é aqui entendida.** Com efeito, como germe que atualiza a potência do virtual, ela é o operador da passagem de uma dimensão da realidade para outra, se lembrarmos que a dimensão atual da realidade é a dimensão do existente, ao passo que a dimensão virtual é a do que existe enquanto potência. Assim, é a informação que permite ao capital global e à tecnociência passarem da dimensão atual da realidade para a sua dimensão virtual. (SANTOS, 2003, p. 18. Grifo nosso)

Para Santos, esse processo se situa no cerne do controle e da colonização das redes pelo capital - em vistas da privatização de todo campo eletromagnético (SANTOS, 2011) - e da integração dos bancos de dados, submetendo as informações relativas aos usuários das redes à exploração e reformulando o chamado direito à privacidade no direito à propriedade dos corpos, corações e mentes. Coerente com o legado probabilístico da ciência cibernética, a ação deste duplo movimento incide não sobre o presente, mas sobre o futuro (SANTOS, 2011; ROUVROY e BERNS, 2015) - sobre os acontecimentos prováveis, possíveis, sobre

uma *"realidade aumentada dotada de memória do futuro"* (ROUVROY e BERNS, 2015) que antecipa a vontade ou a conduta dos sujeitos, permanentemente modelados conforme dados (ROUVROY e BERNS, 2015) e cifras (DELEUZE, 1992) que determinam a relação entre os (in)divíduos e o acesso ou restrição à informação.

Principalmente no contexto do chamado *boom* das empresas ponto.com e de uma crescente narrativa de otimismo em relação às possibilidades das novas tecnologias de comunicação e informação tem-se uma profusão de terminologias que procuram explicar o fenômeno em curso - "revolução informacional", "sociedade em rede", "era da informação" (CAVELTY, 2012; CAVELTY, 2002) - que parecem ter em comum a elevação da informação a um *status* privilegiado da conjuntura em análise. Genericamente, fala-se em um contexto no qual um conjunto de novas tecnologias se localizam no centro de processos de produção de conhecimento e processamento de informações em alta velocidade e através do globo, impactando a comunidade internacional talvez principalmente no que diz respeito à organização do trabalho à globalização da economia (CASTELLS, 2010; CAVELTY, 2012) - o que nas Relações Internacionais com frequência se traduz em termos da transnacionalização da produção e intensificação de dinâmicas de interdependência (NYE, 2004; McCARTHY, 2015).

O alargamento deste fenômeno, contemporaneamente, diz respeito ao que tem sido chamado de quarta revolução industrial, erguida em torno da integração de sistemas complexos, do *big data*, inteligência artificial e a Internet das coisas. O conjunto de técnicas e tecnologias que caracteriza então a fase mais recente deste processo parece alavancar discursos e preocupações que acompanham o desenvolvimento das tecnologias computo-informacionais desde os anos 1990, em particular no que diz respeito à soberania estatal (NYE, 2004; McCARTHY, 2015) e às transformações nas concepções de poder em um mundo no qual a informação enquanto um elemento estratégico parece triunfar sobre a força (NYE, 2004). Em direção contrária, algumas abordagens sugerem que o paradigma da informação no interior de um contexto em constante transformação, em alta velocidade, caracterizado pela mudança e pela instabilidade implica não necessariamente na perda de poder por parte do Estado, mas em um processo de redistribuição constante de relações voláteis de poder entre uma variedade de atores (CAVELTY, 2007). Nessa perspectiva, Cavelty recupera noções de "complexidade", "ordem" e "transformação" como necessários para compreensão do ambiente sociotécnico contemporâneo - noções que por sua vez

retornam à origem da própria lógica que deságua hoje na terminologia da segurança na Era da Informação.

O prefixo *ciber* - ubíquo e por vezes esvaziado de sentido atualmente - se refere a teoria de comunicação e controle de *feedbacks* chamada cibernética, que se difunde a partir da década de 1940, principalmente com o trabalho de Norbert Wiener. Embora sua popularização acompanhe a profusão de terminologias de definição pouco clara e expressões generalizantes, Cavelty (2012) ressalta que se trata de um termo necessariamente vinculado a uma forma de pensamento sistêmico, sendo que *"a noção de ´sistemas´ é absolutamente central no contexto das ameaças cibernéticas e tem diversas ramificações práticas e teóricas para a maneira que o assunto é abordado"* (CAVELTY, 2012, p. 16. Tradução nossa.). Os sistemas cibernéticos, organizados em torno de uma concepção de informação como uma medida de ordem (BOUSQUET, 2009), tinham por objetivo controlar a tendência mecânica à desorganização - ou seja, *"produzir uma reversão temporária e local da direção normal da entropia"* (WIENER apud BOUSQUET, 2009, p. 106. Tradução nossa.). A informação, nesse contexto, passa a ser entendida como um padrão universal, destituído de significado inerente, e tratada como um conceito científico, ocupando espaço central na compreensão da realidade (BOUSQUET, 2009; DAY, 2001).

Em linhas gerais, de forma correlata à lógica do risco e da segurança, a ciência cibernética parte de uma racionalidade probabilística e se interessa pela previsibilidade e controle dos processos, independentemente da natureza maquínica ou biológica de seu mecanismo de referência:

> Os mecanismos cibernéticos, portanto, surgiram naturalmente como os meios pelos quais a ordem poderia ser imposta sobre o caos. Tais mecanismos não se limitariam à solução de problemas de engenharia — Wiener identificaria processos cibernéticos em funcionamento em todos os organismos vivos (...). De fato, um mecanismo cibernético é definido em termos de um processo governado por regras de operação e por um fluxo contínuo de dados aos quais essas regras podem ser aplicadas. Sua função e operação podem, portanto, ser formuladas em termos de relações lógicas e modeladas de acordo com isso por um dispositivo computacional, sendo considerada irrelevante a estrutura específica do mecanismo. (BOUSQUET, 2009, p. 110. Tradução nossa.)

Ainda que tenha perdido popularidade nas décadas seguintes, a cibernética se difunde entre diversos campos do saber, sobretudo na forma de alguns de seus conceitos mais caros - tais como *feedback* e controle - e em sua concepção de informação, até sua mais recente

reconsideração em termos da noção de "complexidade" (CAVELTY, 2012; BOUSQUET, 2009) que, embora reconheça ainda a centralidade da informação para o atual regime tecnocientífico, tem na desordem seu elemento ordenador. Diferentemente da busca pela "solução" para o problema do caos intrínseco à realidade dos mecanismos sociais e técnicos enfrentado pela cibernética de Wiener, associada a formas de organização altamente hierárquicas e centralizadas, os sistemas complexos privilegiam uma lógica de redes descentralizadas e interdependentes, ainda que não abandonem as características de seu predecessor, em uma dinâmica de equilíbrio entre mudança e estabilidade (BOUSQUET, 2009).

Não por acaso, o contexto no qual se inscreve a multiplicação das referidas práticas a todos os campos da vida social corresponderá justamente à ascensão da concepção de informação anteriormente apresentada, na forma do que os estudos da vigilância chamarão genericamente de capitalismo cibernético, ou seja, um sistema totalizante de controle social que depende necessariamente das burocracias do Estado e do mercado para coletar, processar e compartilhar quantidades massivas de informações pessoais, dirigidas ao controle e monitoramento de populações (OSCAR e GANDY, 1993). É em termos de uma lógica de classificação, ou de "triagem cibernética" que Oscar e Gandy exploram o *modus operandi* fundamental das instituições contemporâneas:

> O funcionamento do "ordenamento panóptico" aumenta a capacidade de interesses organizados — sejam eles voltados à venda de sapatos, creme dental ou plataformas políticas — de identificar, isolar e se comunicar de forma diferenciada com os indivíduos, a fim de ampliar sua influência sobre o modo como os consumidores fazem suas escolhas entre diferentes opções. Ao mesmo tempo, (...) atua para aumentar a precisão com que os indivíduos são classificados de acordo com seu valor percebido e sua suscetibilidade a determinados apelos. A mercantilização da informação, por sua vez, intensifica a dependência desses interesses em relação a informações subsidiadas. Na medida em que o ordenamento panóptico, como extensão da racionalização técnica ao campo social do comportamento do consumidor e do comportamento político, depende de uma redução das competências individuais — do mesmo modo que a automação reduz as habilidades dos trabalhadores na fábrica ou no escritório moderno —, o mercado e a esfera política ou pública, tal como os entendemos, são transformados e colocados em risco. (OSCAR e GANDY, 1993, p. 16. Tradução nossa.)

Será justamente sobre esse conjunto de transformações que se desdobram as análises das mutações das práticas da vigilância informacional contemporâneas, exigindo a superação do paradigma do panóptico clássico. Marco elementar não apenas para a crítica às tecnologias

disciplinares, mas para o debate em torno das transformações recentes nas infraestruturas computo-informacionais e nos regimes de visibilidade, as sociedades "pós-panópticas" impõem uma reconfiguração conceitual, sobre a qual o campo dos estudos da vigilância vem se debruçando sistematicamente. A visibilidade, não mais organizada em torno de arquiteturas estatais, passa a ser constituída por algoritmos e redes distribuídas que produzem um ecossistema de monitoramento capilarizado, descentralizado e, paradoxalmente, em geral consentido. Apesar da percepção de esgotamento, que parece ser em geral consenso no campo, David Lyon desabafa: "o panóptico se recusa a ir embora" (2006, p. 4), fato que o autor atribui as possibilidades multifacetadas do conceito ao trazer luz a uma série de problemáticas clássicas da modernidade, a despeito inclusive de, por vezes, ocultar outras ferramentas da analítica foucaultiana que de igual maneira contribuíram para o destrinchar de dispositivos correlatos. Opressivo em seu papel predominante como modelo analítico para os estudos da vigilância (HAGGERTY, 2006, p. 23), o panóptico parece ter atestada sua insuficiência para compreender e analisar fenômenos incompatíveis com seu arcabouço original.

Ao evocar as narrativas iluministas - e em evidente relação com a noção cristã de onisciência em relação a qual estavam em disputa (LYON, 2006) -, a promessa da maximização da visão como forma de controle ainda está no cerne da produção de novas máquinas de visão (VIRILIO, 1994). O fato, entretanto, de que a metáfora do panóptico fora erguida - literal e figurativamente - em torno da prisão, obstaculizando em certa medida a possibilidade de sua generalização, instigou uma geração de autores - Deleuze, Hardt e Negri (2000), Agamben (1997), Bigo (2005) - a se debruçar sobre outros elementos, na forma do que podemos chamar de pós-panoptismo.

Em diálogo, por exemplo, com o campo dos estudos críticos em segurança, Didier Bigo aposta na noção de ban-óptico ao confrontar qualquer percepção do pós-11 de setembro como "estado de exceção" (BIGO, 2016, p. 47), no interior do qual a prerrogativa do soberano de nomear um inimigo público estaria em debate. O ban-óptico, argumenta Bigo, representa um dispositivo que emerge em reação a um contexto de incerteza e desconforto generalizados, reproduzidos na ocasião do atentado às torres gêmeas pelos Estados Unidos e seus então aliados, "convencidos" da ideia de que se instalara um cenário de insegurança global e ameaças de destruição em massa fomentado por redes terroristas e criminosas. As condições estavam postas para a defesa da necessidade de uma articulação de segurança a

nível internacional, na forma de redes de policiamento, da atribuição de funções policiais às forças armadas e deliberada confusão das noções de crime e de guerra. Para o autor, uma "governamentalidade da inquietação" passaria a implementar práticas de excepcionalismo, políticas de perfilamento e contenção e novos imperativos de (i)mobilidade. Bigo conclui:

> O 11 de setembro não é um evento excepcional de violência que redefine as relações da política; ao contrário, representa a regressão de certos governantes a hábitos que revelam a lógica de uma forma de governamentalidade que está profundamente inscrita no que se chama liberalismo — e que, paradoxalmente, gera práticas antiliberais. (BIGO, 2016, p.51. Tradução nossa.)

O controle sobre a circulação, nesse contexto, aparece como consenso entre os cantos do espectro político, em um primeiro momento na forma da narrativa da ampliação da segurança em aeroportos: seja na forma do compartilhamento de dados entre Estados, da criação de novos dispositivos de identificação lançando mão de identidades digitais, biometria, câmeras de circuito interno, reconhecimento facial, enfim - não necessariamente inovadoras em termos de sua adoção ou proliferação (LYON, 2016; BIGO, 2016), o que aparece como alarmante surpresa é a interconexão entre as bases de dados e o consequente alargamento de possibilidades de sua aplicação. É a essa convergência sem precedentes de sistemas de monitoramento que Haggerty e Ericson dão o nome de *surveillant assemblage*:

> Esse agenciamento opera ao abstrair os corpos humanos de seus contextos territoriais, separando-os em uma série de fluxos distintos. Esses fluxos são então reconstituídos em "duplos de dados" específicos, que podem ser examinados e alvo de intervenções. Nesse processo, estamos testemunhando um nivelamento rizomático da hierarquia da vigilância, de modo que grupos antes isentos de monitoramento rotineiro passam agora a ser cada vez mais vigiados. (HAGGERTY e ERICSON, 2000, p. 47)

Em diálogo direto com a contribuição de Deleuze e Guattari, a *assemblage* de Haggerty e Ericson, longe de se referir a uma entidade fixa e estável, representa uma existência em potencial, situada nas intersecções entre uma variedade de infraestruturas de comunicação e informação que podem ser conectadas de diferentes formas. Nesse sentido, os autores propõem a ênfase da análise não em artefatos ou práticas sociais específicas, mas no que identificam como a força motora da vigilância contemporânea: o próprio projeto de integração de sistemas, práticas e tecnologias.

Em um segundo movimento, esse "todo" integrado acabaria, também, produzindo o que os autores entendem como um novo tipo de corpo - nosso *dublê* de dados -, multiplicando

o indivíduo em termos de sua circulação para acesso a recursos e serviços. É sobretudo sobre esse novo corpo dataficado, para Haggerty e Ericson, que intervenções do poder público e de campanhas de marketing passam a se concentrar, de forma que passa a ser pouco ou nada relevante a compatibilidade dessa 'cópia' com seu *dublê* real - pertinente apenas em termos de sua capacidade de fornecer às instituições dados úteis para produzir diferenciações. Mais do que isso, esse fenômeno apresentaria um fenômeno de transnacionalização profunda de nossos *doppelgangers* digitais:

> Os "duplos" estão se tornando uma entidade global — uma espécie transnacional, perpetuamente deslocada, desenraizada culturalmente, estrangeira, que desconhece fronteiras (especialmente diante da natureza supranacional de muitos bancos, companhias de seguros, empregadores, sistemas de segurança, bases de dados etc.). Além disso, a já frágil distinção entre bancos de dados comerciais e arquivos de inteligência torna-se ainda mais tênue quando novas ameaças ou crises de segurança impulsionam uma expansão significativa da securitização. Isso normalmente implica tanto a ampliação dos serviços tradicionais de polícia e inteligência quanto uma maior inclusão de outras agências públicas e privadas em uma rede contínua e integrada de vigilância. (LOS, 2016, p. 78. Tradução nossa.)

Não por acaso, esse cenário responde à tendência operacional da ascensão da informação no centro dos sistemas cibernéticos, cenário no qual os fluxos informacionais passam a ser progressivamente traduzidos em termos de dados - menos relevantes em termos de sua interpretação do que em sua capacidade de circulação. Para Katherine Hayles, este processo se traduz como a transformação da informação em padrões probabilísticos - paradoxalmente - aleatórios, definidos pela distribuição de seus elementos constitutivos (HAYLES, 1999, p.25). Para a autora, é pela coexistência da presença e da ausência, da padronização e da randomização, típicas de sistemas informacionais dos mais diversos, que caracterizam os regimes de visibilidade e subjetivação contemporâneos, situados efetivamente na *interação* entre padrões humanos-maquínicos, e não necessariamente sobre os significantes que porventura emergem dessas interações.

Nessa direção, boa parte dos autores que mobilizam a centralidade da dimensão associativa e integrada das práticas e políticas de vigilância (WOOD, 2013; HAGGERTY e ERICSON, 2000; MATTELART, 2010) recorrem ao argumento clássico de A. Galloway (2006) segundo o qual o caráter distribuído e em rede das chamadas sociedades do controle (DELEUZE, 1992) seria o elemento que constitui efetivamente a atualização da metáfora do Panóptico à luz da ascensão das tecnologias computo-informacionais. Nesse enquadramento,

Puar (2012) e Wood (2013) sugerem que a terminologia do *controle* de Deleuze corresponderia, de fato, a *segurança* de Michel Foucault, marcada sobretudo pelas novas configurações espaço-territoriais típicas da segunda metade do século XX (WOOD, 2013), não mais necessariamente circunscritas pela figura do Estado Nação. Concordam, ao mesmo tempo, com a interpretação deleuziana sobre o deslocamento, nas sociedades do controle, da intervenção governamental para o controle de fluxos - principalmente, fluxos de dados:

> Houve, assim, uma fragmentação do sujeito individual moderno em uma forma dividida, ou em múltiplos "dividuais". Isso se distancia da simples quantificação que fundamentava a segurança biopolítica em sua formulação inicial. Essa qualidade artefactual e híbrida da sociedade de controle (...) permite argumentar que a vigilância contemporânea tornou-se desterritorializada e opera como uma rede heterogênea de elementos que se expandem de modo rizomático. (WOOD, 2006, p. 319. Tradução nossa.)

Sobre a dimensão primordialmente informacional da vigilância contemporânea, Fernanda Bruno recorrerá ao termo *vigilância distribuída*, herdeira ao mesmo tempo dos sistemas modernos de coleta e classificação de informações e das transformações trazidas pelas tecnologias digitais. Bruno (2013) concordará com as perspectivas supracitadas em termos da insuficiência do argumento da hipertrofia do panóptico como caracterização contemporânea do fenômeno da vigilância e enfatiza, como Wood e Haggerty, que as rupturas mais substanciais em relação às práticas e políticas de vigilância modernas dizem respeito ao seu modo de funcionamento, e não a sua intensidade. Ressaltando o elemento aparentemente contraditório da noção de *distribuição*, a autora recorda se tratar, ao mesmo tempo, de uma referência à natureza reticular e heterogênea das formas contemporâneas da vigilância, e de uma sinalização direta à *"experiência de distribuição em ambientes e redes digitais de comunicação"* (BRUNO, 2013) típicos da web 2.0, em seu potencial simultâneo de subversão e retroalimentação dessa mesma arquitetura. Trata-se, ao mesmo tempo, de uma noção "*que espraia por muitos e diversos agentes, tecnologias, contextos, práticas, sem constituir uma atividade ou processo unificado que possa ser plenamente atribuído a intenções de um centro de ordenação"* (BRUNO, 2013.).

Bruno resumirá sua proposição em torno de sete atributos, dentre os quais a descentralização, diversificação, indiscernibilidade, funcionalidade, e a delegabilidade. A sexta característica elencada pela autora, por sua vez, indica a extrapolação das práticas de vigilância distribuída para além de circuitos de controle e segurança e seu alastramento por

uma variedade de contextos sociais de natureza cotidiana, inclusive na forma de dispositivos de automonitoramento e otimização da performance voltados a atividades de trabalho e saúde, entre outros. Por último, o sétimo atributo se refere ao que a autora chama de "impulso participativo" das práticas de vigilância distribuída, mobilizadores de modos de atenção vigilantes dos sujeitos uns sobre os outros, sob o marco do exercício da cidadania. Ao lado da gramática do risco e da segurança, a autora aponta para os dispositivos de visibilidade como uma via de legitimação da vigilância, incrementados pelas tecnologias de comunicação em massa e as suas subsequentes mutações no campo do ver e do ser visto:

> Seja na Internet e nos diversos dispositivos que constituem o ciberespaço, seja na própria televisão, assistimos a um crescente retorno da exposição do indivíduo comum à visibilidade, agora residente não mais nas instituições disciplinares, mas nos ambientes telemáticos (...) Nem panóptico nem sinóptico, mas um modelo reticular e distribuído onde muitos vigiam muitos ou onde muitos veem e são vistos de variadas formas. (...) a vigilância contemporânea, seus dispositivos, seu modo de funcionamento e suas vias de legitimação são fortemente atravessados por esses jogos do ver e do ser visto, no seio dos quais as subjetividades encontram um domínio privilegiado de investimentos e cuidados. Não é portanto de se surpreender que para esta subjetividade a vigilância, considerando suas múltiplas formas e significações atuais, apresente-se como aceitável, chegando a ser por vezes requerida (BRUNO, 2013, p. 47)

A permeabilidade dos processos descritos pela autora, evidentemente, dialoga com a condição das sociedades informacionais anteriormente explorada, impulsionada ainda mais pelo advento da Internet 2.0, aquela designada para abarcar aplicações de comunicação tais como blogs, microblogs (como o Twitter) e plataformas de compartilhamento, em geral (FUCHS, 2017; TERRANOVA, 2013). Em princípio acompanhada de uma narrativa de descentralização radical, intensa participação do usuário que teria pleno controle de seus próprios dados e "inteligência coletiva", os idealizadores da web 2.0 a pretendem - pelo menos no âmbito do discurso - distinta de tudo o que precedera. Fruto do contexto imediatamente posterior à crise da bolha da internet nos anos 2000, este processo de inovação fortifica promessas de democracia e de uma "nova" economia, erguida sobre valores de inclusão, ao mesmo tempo em que promove certo esforço de superação da crise e de aberturas de novos modelos de acumulação para uma então decadente indústria digital.

A esse respeito, algumas análises se ativeram sobre características, de fato, participativas das novas plataformas em ascensão, procurando enfatizar a dimensão de colaboração supostamente inscrita nelas, compreendendo esse contexto como um potencializador da conectividade humana como um valor universal (VAN DIJCK, 2013) e o ciberespaço como um território compartilhado - a partir, por exemplo, da noção amplamente circulada no mercado de *user-generated content*, ou seja, "conteúdo gerado pelo usuário". Por outro lado, estavam também em pauta preocupações alinhadas com as novas possibilidades de mercado assinaladas, mais tarde, por Zuboff - como exploramos no capítulo 2,

> Desde pelo menos 2004, a Internet, e mais especificamente a Web, testemunhou uma mudança notória e controversa do modelo da página da web estática para uma web social ou modelo da Web 2.0, onde as possibilidades dos usuários interagirem com a web se multiplicaram. Tornou-se muito mais fácil para um leigo publicar e compartilhar textos, imagens e sons. Uma nova topologia de distribuição de informações surgiu, baseada em redes sociais "reais", mas também aprimorada por conexões casuais e algorítmicas. Comércio, publicidade e jogos constituem os modelos de negócios pelos quais as plataformas de redes sociais monetizam a atenção dos usuários. Junto com a crescente relevância da comunicação móvel e sem fio, esta mutação na evolução contínua da web remodelou profundamente sua cultura. Muitos argumentaram, no entanto, que esta nova fase viu uma incorporação ainda mais intensa da internet com a cultura corporativa e capitalismo cognitivo (Terranova e Donavan, 2013, p. 297. Tradução nossa.)

Fuchs, na mesma direção, ressalta o que entende pela dimensão ideológica do suposto paradigma participativo da web 2.0 (FUCHS, 2011), dimensão que ocultaria a emergência de uma categoria híbrida entre produtor e consumidor, associada a uma operação permanente de coleta da inteligência coletiva de todos os envolvidos (BRUNS, 2008; FUCHS, 2017), que, por sua vez, dependeria da difusão de narrativas sobre a cultura da participação da Internet e das mídias sociais para se consolidar. A habilidade intensa de compartilhamento coletivo de dados e informações, que para algumas análises representaria um processo de democratização da produção de conhecimento, estaria na própria fundação das transformações produtivas que Zuboff reconhece pelos processos de extração e análise de dados do usuário, traduzidos, por exemplo, por Terranova (2004) em termos de exploração de trabalho gratuito. Fuchs resume:

> Ainda que todos possam produzir e difundir informações, a princípio, com facilidade por meio da Internet por meio de seu sistema descentralizado de comunicação, nem toda informação é visível de igual maneira ou recebe a mesma atenção. O problema no fluxo de

> informações no ciberespaço está em como nesse oceano informacional usuários têm sua atenção atraída para informação (...) Há uma certa estratificação online de uma economia da atenção pela qual as marcas registradas dos atores mais poderosos operam como poderosos símbolos que auxiliam os portais de certas organizações a acumular atenção. (...) Plataformas corporativas da web 2.0 atraem a ampla maioria de usuários. (FUCHS, 2011, p. 277. Tradução nossa.)

A economia da atenção a qual se referem, de uma forma ou de outra, diversas destas análises (FUCHS, 2011; FUCHS, 2017; ZUBOFF, 2019; TERRANOVA, 2004), diz respeito à necessidade compartilhada pelas plataformas corporativas de manter seus usuários online pela maior quantidade de tempo possível, a fim de potencializar, conforme Fuchs (2017), a acumulação de capital pelas mídias sociais corporativas. Sobre esse cenário, parte relevante da literatura se concentrará na capacidade digital de identificação de sujeitos de maneira direta ou indireta, tensionando categorias clássicas como anonimato e privacidade.

Bruno (2013) enfatiza, entretanto, que essa leitura, embora pertinente, contribui para obscurecer mecanismos que não se organizarão primordialmente em torno da identificação, mas em registros distintos — infraindividuais ou supraindividuais —, nos quais o dado circula como vestígio ou rastro, e não como representação nominal do sujeito. Nessas práticas, o que importa não é tanto a figura do indivíduo reconhecível, mas a agregação e a recomposição de padrões que permitem descrever, prever e modular. O foco se desloca para o funcionamento de algoritmos de correlação e redes de associação que produzem inteligibilidade a partir de fragmentos dispersos, respondendo não à lógica da vigilância que vigia “alguém”, mas a do monitoramento que rastreia fluxos e desvios. Esse deslocamento, por sua vez, revela um tipo de poder que se estrutura não pela nomeação e exclusão de sujeitos, mas pela captura contínua dos traços digitais deixados pela interação em ambientes conectados. Identificar passa a ser apenas uma das possíveis etapas de um processo mais amplo, em que o essencial é a produção de conhecimento operacional sobre comportamentos e populações. Trata-se, portanto, de um regime de governo em que o rastro digital assume centralidade, relativizando a primazia da identidade civil como condição para vigilância e controle. A esse regime, Rouvroy e Berns darão o nome de governamentalidade algorítmica:

> Uma espécie de racionalidade (a)normativa ou (a)política que repousa sobre a coleta, agregação e análise automatizada de dados em quantidade massiva de modo a modelizar, antecipar e afetar, por antecipação, comportamentos possíveis (ROUVROY e BERNS, 2015, p. 42)

Seu traço distintivo, para os autores, reside na independência da imposição de normas ou de orientações explícitas do Estado, fundamentada pelos inúmeros vestígios digitais deixados por indivíduos em suas práticas cotidianas *online*, que, uma vez coletados e processados, tornam-se matéria-prima para a gestão social. Nesse arranjo, a lei e a normatividade perdem o protagonismo, cedendo espaço a um regime em que o cálculo e a quantificação substituem os instrumentos clássicos tanto da política quanto da estatística (Santos, 2019, p. 4). Em vez de confirmar pressupostos, ela produz as próprias classificações e hipóteses a partir do processamento massivo de dados. Dessa perspectiva, o poder dos algoritmos estaria menos em validar concepções existentes, mas sobretudo em criar novas formas de ordenação e inteligibilidade do social, fundadas diretamente nos rastros informacionais. Podemos entender esse arranjo em sua natureza multifacetada, que opera simultaneamente como dispositivo *"epistêmico, individualizante, taxonômico e performativo"* (BRUNO, 2013)

Em primeiro lugar, situam-se os métodos de rastreamento, monitoramento contínuo e armazenamento sistemático de dados - ou, para Rouvroy e Berns, nos processos de *dataveillance*. Em seguida, aparecem os regimes de categorização que transformam rastros dispersos em bases de conhecimento organizadas - ou, *datamining* (Rouvroy e Berns, 2015.). A terceira dimensão é marcada por processos que individualizam os sujeitos, vinculando-os a perfis e identidades digitais singulares, na forma de tecnologias de perfilamento, ou *profiling*. Por fim, em sua camada performativa o controle se antecipa às condutas, orientando preferências, escolhas e trajetórias futuras por meio de mecanismos proativos de gestão (Bruno, 2013). Rouvroy (2020) observa que a lógica algorítmica parte do pressuposto de que a melhor forma de assegurar o futuro é certificar-se dele de antemão, no presente, transformando o *incerto* em *necessário*. Nesse horizonte, a governamentalidade algorítmica busca neutralizar a contingência, suprimindo a abertura ao acaso e à multiplicidade, dispensando a imaginação e a incerteza como elementos constitutivos da vida social.

Ao reduzir o espectro de futuros possíveis a um único caminho calculado, elimina-se a potência criadora do inesperado, de modo que falhas e desvios deixam de existir como possibilidades. O efeito é um processo de normalização radical, que tende a sufocar a disparidade e que converte a subjetividade em matéria-prima lucrativa, ameaçando corroer a

própria ideia de autonomia (Couldry e Mejias, 2019). Localizando o agir humano em um mundo governado por dispositivos que comprometem qualquer forma de integridade do *self*, Couldry e Mejias alertaram para o risco de esquecimento progressivo dos hábitos, normas e práticas associados à liberdade – constituindo sujeitos cada vez menos aptos a reivindicá-la.

Zuboff (2020), em proposição semelhante, sublinha que a liberdade exige incerteza, dado que seria justamente no espaço da imprevisibilidade que a promessa – fundamento dos contratos e da vida em comum – pode ser enunciada. O regime algorítmico, ao contrário, desenha um mundo de previsibilidade total, no qual a própria ideia de contrato se dissolve, sem haver necessidade de compromisso ou espaço para escolhas. Esse "não-contrato" gera um estado de entorpecimento e de obediência quase automática assumindo, no limite, a forma de um novo behaviorismo, não mais em torno de estímulos laboratoriais, mas do acúmulo massivo de dados digitais. Rouvroy (2020) sintetiza, sobre esta hipótese, que o "behaviorismo de dados" se ancora na crença de que a simples correlação estatística, sustentada por grandes volumes de informação, é suficiente para antecipar condutas humanas, tornando desnecessária qualquer consideração sobre intenções, significados ou causalidades. Nesse regime, não se trata fundamentalmente de um indivíduo ser constrangido a abrir mão de sua privacidade ou forçado a aderir a um padrão de conduta. O que vemos é uma espécie de descentramento: o sujeito não interage mais com uma norma que lhe é exterior e contra a qual poderia insurgir-se, mas com uma normatividade difusa, inscrita no tecido mesmo de suas interações digitais.

É nesse sentido que Antoinette Rouvroy (2021) argumenta que a governamentalidade algorítmica "contorna" o sujeito. O projeto individual – marcado por hesitações, falhas, transformações – dissolve-se diante de um dispositivo que antecipa e ajusta trajetórias, dispensando a dimensão da escolha e da resistência. Essa lógica, como nota Berns (2020), implica uma verdadeira inversão do funcionamento histórico da norma. No direito clássico, a norma era sempre binária: poderia ser obedecida ou violada, admitindo a insubmissão como horizonte, ainda que punida, sob a hegemonia do poder soberano. No contexto algorítmico, esse movimento atinge seu ponto mais radical: as normatividades contemporâneas passam a se apresentar como técnicas, deixam de "governar o real" e passam a ser "extraídas do real", ajustando-se às regularidades estatísticas que emergem da captura permanente das condutas. Trata-se, em suma, da constituição de um ambiente que se modela continuamente às propensões dos indivíduos. Governa-se, como argumenta Berns (2020), não a partir de

decisões conscientes, mas recolhendo o que já está aí, extraindo inteligibilidade da atividade humana em estado bruto, conferindo às tecnologias de governo a aparência de simples registro ou acompanhamento do real e esvaziando gradativamente os espaços de resistência típicos do século passado.

A predição algorítmica, hoje disseminada em diversos setores, exemplifica com clareza o tipo de intervenção que caracteriza a governamentalidade do presente, reduzindo incertezas em campos como investimento financeiro, publicidade, políticas de saúde ou estratégias de segurança, e produzindo efeitos diretos sobre o espaço de ação dos indivíduos. Os perfis resultantes do processamento de rastros digitais não são representações neutras de identidades, mas matrizes que projetam possíveis trajetórias, de consumo, acesso a serviços ou probabilidade de risco e perigo. O que está em jogo, portanto, não é tanto a subjetividade consciente, mas a própria ação como campo de manipulação e antecipação (Bruno, 2013; Gandy, 1993).

O perfilamento é, assim, uma tecnologia de triagem, de regulação do acesso ao consumo, a direitos, bem-estar ou cidadania. As recompensas e sanções derivadas dessa filtragem não se organizam em torno da subjetividade ou da interioridade, mas em torno do acesso diferencial a circuitos invisíveis de inclusão ou exclusão, performando realidades de pertencimento e marginalização sem recurso à força direta. Para Bruno (2013), o saldo final é uma cultura de controle que não se apoia prioritariamente na imposição de valores normativos, mas na mobilização contínua de práticas sociais segundo critérios de otimização que encorajam tendências desejáveis e inibem aquelas consideradas nocivas. O exercício de poder se dá sob a forma de parceria e corresponsabilidade, em que seríamos induzidos a participar ativamente de nossa própria vigilância, assumindo riscos e praticando o autocontrole. O caráter preditivo do perfilamento, portanto, encontra ressonância direta em uma cultura mais ampla de performance (Bruno, 2013), na qual os dispositivos de vigilância operam simultaneamente como mecanismos de capacitação – oferecendo informações e métricas para escolhas – e instrumentos de contenção – limitando alternativas e horizontes de futuro.

Em síntese, procuramos até aqui recuperar as características distintivas da vigilância contemporânea, localizando como suas práticas, inicialmente vinculadas à burocratização estatal e à expansão capitalista, deslocaram-se progressivamente para regimes informacionais

distribuídos em escala planetária. O que se observa é a permanência de uma racionalidade orientada para a segurança - ou seja, para o controle dos fluxos e a antecipação das condutas -, mas constantemente reformulada por contextos sociotécnicos em rápida mutação.

Importante ressaltar que nessa nova ecologia de visibilidade, a privacidade não desaparece. Pelo contrário: torna-se elemento estratégico, redefinido constantemente por disputas entre regulação estatal, interesses corporativos e práticas sociais, representando talvez o objeto de regulação primordial para legitimação ou obstacularização dos fluxos informacionais dos quais, em última instância, dependem as *assemblages* da vigilância. Essa trajetória, então, prepara o terreno para compreendermos como tais mutações não se restringem a âmbitos técnico-domésticos, mas se cristalizam em pactos normativos e práticas multilaterais que consolidaram a vigilância como uma gramática incontornável das relações internacionais no século XXI, conforme procuraremos abordar na próxima seção.

1.3 A política internacional da vigilância: uma gramática em três tempos

Se a racionalidade da segurança como tecnologia de governo encontra, nos dispositivos tecnopolíticos contemporâneos, sua expressão mais refinada na modulação algorítmica e na gestão estatística do risco, é no plano internacional que essa lógica se manifesta de forma estruturante. Em continuidade ao discutido nos itens anteriores, a vigilância não pode mais ser apreendida só em termos de um fenômeno doméstico ou disciplinar, mas como parte de um arranjo transnacional que conjuga a informatização profunda de todas as dimensões da vida social, associada a rápida multiplicação de infraestruturas descentralizadas. Nesse regime, o visível é aquilo que circula por redes transnacionais, mas cuja legibilidade e uso político permanecem concentrados em atores com capacidade de processamento técnico e normativo (Couldry & Mejias, 2019). Reforça-se, aqui, a pertinência de se conceber uma política internacional da vigilância não mais como um epifenômeno das r(R)elações i(I)internacionais, mas como um campo no qual dispositivos sociotécnicos, práticas securitárias e racionalidades específicas se articulam de forma imanente, como pretendemos desenvolver nos próximos capítulos.

Embora o diálogo entre os Estudos da Vigilância e as Relações Internacionais seja evidente, por exemplo, na literatura sobre operações de inteligência, espionagem, contra insurgência e vigilância militar (Dandeker, 1990), é apenas a partir do 11 de Setembro e mais ainda com o episódio Snowden de 2013 - que o encontro entre ambos os campos se torna

progressivamente frutífero. Com a popularização do computador pessoal e da Internet comercial, ao lado da proliferação de reflexões em torno das sociedades de informação é que as RI, de fato, testemunham um salto em sua produção teórico-conceitual no que diz respeito à dimensão tecno-informacional da política internacional, assumindo de forma constitutiva a vigilância como forma de ordenamento primordial da realidade planetária contemporânea. Ainda que não possam ser tratados em termos de causalidade direta, a literatura ressalta o encontro conveniente entre demandas, investimentos e experiências governamentais, acadêmicas e militares em torno principalmente do campo da cibernética e da segurança da informação - por exemplo na forma da *Defense Advanced Research Projects Agency* (DARPA) - e a aceleração da difusão de práticas e políticas de vigilância que posteriormente apagaram as fronteiras entre a vida civil e militar,

> O potencial para formas abrangentes de vigilância foi percebido relativamente cedo, quando estrategistas militares norte-americanos, durante o período da Guerra Fria, trabalhavam em direção ao que concebiam como um "mundo fechado" de controle total da informação — uma configuração que combinava cibernética e vigilância para recriar o globo como um espaço defensável e seguro. Juntamente com a criação de múltiplos sistemas orbitais de vigilância por satélite, esse impulso do "mundo fechado" também levou, no final da década de 1960, à combinação entre computação e telecomunicações em um sistema eletrônico de comunicação distribuído e seguro, baseado em comutação de pacotes — o ARPAnet, que viria a constituir as bases da Internet. (MONAHAN e WOOD, 2018, p. 150. Tradução nossa.)

Embora, como afirmam os autores, os processos de inovação não tenham sido necessariamente determinantes nas formas adquiridas pelas práticas de vigilância da segunda metade do século XX, nota-se a sinergia significante (Monahan e Wood, 2018) na experimentação interdisciplinar típica do campo da cibernética e a potencialização de novas experiências nos órgãos de inteligência do Estado. É, num primeiro momento, o investimento em tecnologias como computadores, satélites e telecomunicações que sustentaria a posterior consolidação de uma rede global de monitoramento contínuo.

Esforços de inteligência compartilhada - como apareceriam mais tarde no caso do "Five Eyes[1]" - estavam em gestação desde o final da Segunda Guerra Mundial entre os

[1] Se refere à aliança de inteligência formada entre Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia, precedido pelo UKUSA Agreement (1946), um tratado para cooperação em interceptação de comunicações, que gradativamente incorporou outros países da Commonwealth, constituindo a formação atual do grupo. Em síntese, a aliança se refere à cooperação em vigilância e inteligência de sinais (SIGINT), interceptação de comunicações eletrônicas — como telefonemas, e-mails, fluxos de dados e satélites. O Five Eyes opera como uma rede de compartilhamento de informações estratégicas, em que cada país é responsável

Estados Unidos, Grã Bretanha e parte da Europa Ocidental, marcada por uma variedade de operações anti soviéticas.

Em *War in the Age of Intelligent Machines* (1991), Manuel DeLanda mobiliza referenciais da ciência cibernética, da teoria dos sistemas complexos e da teoria da evolução ao apontar que a guerra estaria se tornando, no contexto da virada para a segunda metade do século XX, um sistema auto-organizado, baseado em processos de inteligência distribuída, semelhantes aos encontrados em colônias de insetos ou no próprio sistema imunológico humano. A partir dos sistemas modernos de radares, sensores e computadores - pano de fundo para um verdadeiro "sistema nervoso militar planetário", o autor propõe uma descrição tecnogenética da guerra, expressando efetivamente um processo co-evolutivo entre humanos e máquinas que, por sua vez, respaldaria formas de governo. O autor também descreve a emergência do *panspectron* norte-americano - que ampliaria a metáfora do Panóptico para todas as frequências do espectro eletromagnético, se referindo a multiplicação de fazendas de antenas, satélites espiões e interceptações de tráfico de comunicações a cabo, culminando em um cenário de quantidades massivas de informação sendo coletadas a todo tempo (DeLanda, 1991). Ao lado do crescimento vertiginoso de iniciativas do setor privado (Hayes, 2009), De Landa materializa na figura do *panspectron* uma ferramenta maquínica de governança global da paz e da guerra, antecipando a amplitude adquirida pelas redes transnacionais de vigilância contemporâneas. Um novo complexo militar-industrial da vigilância articularia, nesse contexto, forças militares, técnicas e corporativas em rede, fortalecendo seu papel como instrumento de poder.

Com o fim da Guerra Fria, esse processo se consolida em um complexo informacional-militar caracterizado pela transferência de percepções de risco e ameaça no campo da informação para todos os campos da vida social, sendo transferidas de igual maneira as competências, capacidades técnicas e soluções de mercado voltadas para a vigilância total (Monahan e Wood, 2018). Ao longo da primeira década dos anos 2000, as Relações Internacionais e os ESI se percebem atravessados pela necessidade urgente de uma recuperação sistemática das práticas contemporâneas de monitoramento e vigilância (Bigo et

pela cobertura de uma determinada região, compartilhando dados posteriormente com os demais membros. Esse arranjo permaneceu relativamente desconhecido até as revelações de Edward Snowden em 2013, que demonstraram a coordenação do Five Eyes de programas de vigilância em massa, como o PRISM (coleta de dados de usuários de grandes empresas de tecnologia) e o XKeyscore (rastreamento de atividades online).

al, 2014.) à luz da incontornável relevância adquirida pela Internet no mesmo período. Bigo et al., a esse respeito, alertam para a rápida intensificação da transnacionalização das agendas de segurança nacional que encorajaria a universalização de práticas de policiamento preditivo e da interpretação de todo e qualquer usuário da rede como um suspeito em potencial. Os autores resumem:

> As práticas de vigilância em larga escala realizadas pela NSA e suas congêneres devem, portanto, ser compreendidas (...) como indicadores de uma transformação muito mais ampla que afeta o modo como funcionam as fronteiras da segurança nacional. Isso se deve à conjunção de três processos que se entrelaçaram: **transnacionalização, digitalização e privatização**. Essa conjunção produz um efeito abrangente de **dispersão**, que desafia a própria ideia de uma *razão de Estado* conduzida por um "Estado" no qual o governo determina os interesses e a segurança nacionais e solicita a seus próprios serviços que atuem de acordo com essas diretrizes. (...) Ao contrário, o que observamos é a **transformação da razão de Estado** por meio do surgimento de uma **razão de Estado digitalizada**, desempenhada por um complexo heterogêneo de profissionais que lidam com informações sensíveis e que hibridizam atores públicos e privados. A natureza transnacional da coleta de informações que atravessam as fronteiras dos Estados **dissocia o caráter discursivo e homogêneo dos interesses de segurança nacional**, ao mesmo tempo em que **reconstrói um agregado de profissionais**. Esses profissionais trocam informações por meio de tecnologias digitais, produzem inteligência de acordo com seus próprios interesses e desprezam a ideia de que os direitos de todos os usuários da Internet possam impor limitações a seus projetos. (BIGO et al., 2014, p. 126. Grifos nossos. Tradução nossa.)

O suposto consenso liberal em torno da aceitação limitada de práticas de vigilância em Estados democráticos (Bigo et al., 2014; Haggerty e Ericson, 2000) é abruptamente rompido pelas medidas adotadas em resposta aos atentados às torres gêmeas e, posteriormente, escancarado pela revelação do programa PRISM, situando nosso cenário na convergência entre a governança e a segurança que nos interessa na presente reflexão. Nosso primeiro ponto de inflexão para esse processo aparece como incontornável na literatura da vigilância do Século XXI, enfatizando as consequências do 11 de setembro em termos da elucidação de um conjunto de tendências em vigilância estatal que, até então, pareciam se desenvolver discretamente. Lyon destaca que o 11 de setembro não inaugurou as sociedades de vigilância, mas tornou mais evidente um processo já em andamento. Segundo ele, práticas de videomonitoramento, que antes eram tratadas de forma periférica pela mídia, passaram a ocupar espaço central no debate público, ao mesmo tempo em que a participação dos

cidadãos como colaboradores da segurança foi retomada como estratégia de legitimação. (LYON, 2003).

Ao mesmo tempo, o episódio com frequência foi tratado também como uma oportunidade especial para o alargamento de práticas de "controle social" (Lyon, 2003; Bigo et al., 2014) que estavam em curso, até então relativamente impopulares no contexto da globalização liberal. Os aparatos para mineração de dados em larga escala, já utilizados para fins comerciais, encontraram no combate ao terrorismo uma justificativa legítima para sua ampliada e acelerada adoção no campo da segurança (inter)nacional. Se antes dos atentados de 11 de setembro, a aliança entre segurança e vigilância não ocupava papel central no debate político, rapidamente passaram a dominar a agenda pública, em torno por exemplo de tecnologias como biometria e câmeras de CCTV, apresentadas como respostas imediatas à ameaça terrorista, convertendo a crise em uma oportunidade para expandir e intensificar sistemas já existentes. Infraestruturas de monitoramento e suas capacidades latentes, portanto, tornam-se nesse contexto rapidamente mais ostensivas.

Mais do que o alargamento do monitoramento civil no território norte-americano, o 11 de setembro implicou de igual maneira na aceleração da transnacionalização de burocracias de vigilância e no robustecimento da coordenação global em torno de serviços de segurança nacional. Bigo (2014) recorda que, nesse contexto, a narrativa securitária começa pela aviação civil, com a presença de agentes armados em aeronaves e o fortalecimento de dispositivos de triagem em aeroportos. Organizada em torno da construção de um regime de identificação contínua e cada vez mais invisível, apoiado por tecnologias e serviços ofertados pelo mercado da segurança, trata-se de uma lógica que assume a invisibilidade do controle como ponto crucial, em sociedades marcadas pela narrativa da globalização, de indivíduos que prezam pela fluidez. Tal racionalidade, segundo o autor, projeta a expansão do modelo aeroportuário para outros espaços coletivos, em nome de uma transparência ambígua: não se esconder da polícia e, ao mesmo tempo, proteger-se de ameaças futuras.

Embora o controle da circulação de tenha se expandido, os controles mais coercitivos recaem, evidentemente, sobre alvos específicos, tendo os atentados contra as torres gêmeas, nesse sentido, legitimado práticas de perfilamento de condutas consideradas de risco, sobretudo as associadas à mobilidade. Nesse contexto, a reação política ao atentado reforçou estratégias preventivas e preditivas, voltadas a antecipar ameaças futuras, apoiando-se em

grandes bancos de dados transnacionais que reúnem tanto informações verificadas quanto rumores e fragmentos de inteligência. Para Bigo, teríamos aqui a combinação de tecnologias de ponta — como biometria, DNA e bases digitais — com uma racionalidade quase astrológica, típica dos discursos de segurança de certas elites políticas, que confiam no corpo como portador de uma verdade capaz de revelar comportamentos futuros (Bigo et. al, 2014)

Se o 11 de setembro inaugura a gramática da vigilância ampliada, as revelações de Snowden sobre o Programa PRISM em 2013 marcam nossa segunda inflexão, para uma percepção pública de vigilância "em massa". A partir de um deslocamento do *locus* privilegiado de coleta e controle dos espaços de circulação de populações para *os espaços de circulação de dados*, o PRISM incluiu práticas de interceptação em trânsito - de dados oriundos de fibras ópticas subterrâneas conectando os Estados Unidos ao resto do mundo - em cooperação com empresas de telecomunicações, práticas de interceptação de dados armazenados - em cooperação com o GCHQ britânico e com servidores norte-americanos de *big techs* como a Apple, a Meta, o Google, a Microsoft, entre outros -, e práticas de instalação de *spywares* em computadores pessoais. Lyon (2015) resume

> A vigilância em massa não apenas se expandiu para além da vigilância direcionada realizada pela NSA dentro dos Estados Unidos, mas também nas suas contrapartes de inteligência ao redor do mundo. Isso se torna cada vez mais evidente em outros domínios da vigilância também, como veremos. As fronteiras entre "vigilância em massa" e "vigilância direcionada" tornaram-se profundamente borradas.Quando os dados são coletados em larga escala — abrangendo amplos segmentos de uma determinada população — com o objetivo de identificar quem pode ser uma "pessoa de interesse", o ponto em que a vigilância "em massa" se transforma em vigilância "direcionada" é, na melhor das hipóteses, impreciso. Essa identificação é feita por meio de algoritmos — os códigos computacionais que orientam como os dados são organizados —, a fim de criar conexões e revelar correlações que podem ou não resultar em uma pista concreta. (LYON, 2015, p. 60. Tradução nossa.)

Nessa direção, Bigo et al. (2014) argumentam que as práticas contemporâneas de vigilância em larga escala, como as conduzidas pela NSA e por suas contrapartes internacionais, transformaram profundamente os contornos da segurança nacional, de modo que esta já não pode mais ser entendida como restrita ao âmbito estatal. A transnacionalização da coleta de informações, combinada à digitalização e a participação de atores privados, teria gerado efeitos paradoxais sobre os parâmetros das práticas de segurança - enquanto as fronteiras nacionais se tornam difusas, também se diluem as linhas que distinguem atuação policial de inteligência, deslocando o foco de uma segurança baseada em certeza jurídica e

controle limitado de dados para abordagens preventivas, preemptivas e preditivas sobre grandes volumes de informação. A distinção entre categorias "estrangeiro" e "doméstico" é diluída progressivamente, transformando a linha soberana que antes as separava em algo semelhante a uma "fita de Möbius"[2]. Essa mudança evidencia a emergência de uma nova "razão de Estado digitalizada", conduzida por um complexo heterogêneo de profissionais de inteligência, híbrido entre setores público e privado, cuja atuação transnacional redefine, também, a percepção e a fonte dos interesses entendidos como nacionais. Em síntese, os autores sugerem que o conceito clássico de segurança nacional teria sido colonizado pelos altos escalões de agências de inteligência, cada vez mais autônomas em nível transnacional.

Nesse contexto, Estados, movimentos sociais e indivíduos atuam reinterpretando os significados de soberania, cidadania, segurança, liberdade - e, claro, privacidade. No caso do Brasil, as revelações de Snowden sobre a vigilância da NSA — incluindo a interceptação do telefone da então presidenta Dilma Rousseff, a interceptação de dados da Petrobras e as evidências de vigilância indiscriminada de cidadãos brasileiros — desencadearam respostas múltiplas em diferentes arenas, como o adiamento de visitas oficiais aos Estados Unidos e a inclusão dos direitos à privacidade na agenda da Assembleia Geral da ONU, resultando na introdução de uma resolução apoiada pela Alemanha, que, embora não mencionasse diretamente as intrusões norte-americanas, censurava implicitamente as práticas de vigilância em massa. A adoção de um vocabulário universal nesse cenário internacional buscava garantir a atualização do reconhecimento da privacidade como direito humano, ao mesmo tempo em que desestabilizava o núcleo das práticas de vigilância, cuja preocupação central é o "sujeito dataficado", cuja existência e direitos são condicionados por suas condutas. Nesse regime de razão de Estado digitalizada, os direitos e prerrogativas individuais passam a ser determinados por suas relações, proximidade ou distância a alvos de interesse estratégico, contrastando, é claro, com as premissas cosmopolitas que pareceram sustentar as campanhas por direitos cibernético-universais promovida por países como Brasil e Alemanha.

[2] Uma fita de Möbius é uma superfície geométrica que possui apenas um lado e uma única borda, criada ao pegar uma tira de papel retangular, dar meia volta em uma das extremidades e colar as pontas; ao percorrer sua superfície, é possível cobrir toda a extensão sem nunca atravessar uma borda, e ao seguir a borda com o dedo, ela leva de volta ao ponto de partida sem encontrar outra, revelando propriedades contraintuitivas que desafiam a noção de "lado de dentro" e "lado de fora". Na metáfora utilizada por Didier Bigo, a fita de Möbius ilustra como categorias aparentemente opostas, como "estrangeiro" e "doméstico" ou "dentro" e "fora" do Estado, se entrelaçam continuamente.

As consequências imediatas do episódio Snowden podem, de igual maneira, ser rastreadas às arenas multilaterais. Em 2013, a Assembleia Geral da ONU aprovou, por iniciativa do Brasil e da Alemanha, a Resolução 68/167, que estabeleceu pela primeira vez o "direito à privacidade na era digital" como tema específico da agenda internacional. No ano seguinte, o Alto Comissariado das Nações Unidas para os Direitos Humanos (ACNUDH) publicou o relatório A/HRC/27/37, no qual diagnosticava lacunas normativas e deficiências de fiscalização que dificultavam a avaliação da legalidade e da proporcionalidade das práticas de interceptação e coleta de dados.

Esse processo inaugurou um ciclo de relatórios periódicos e debates no Conselho de Direitos Humanos, no qual a privacidade deixou de ser um direito residual para se consolidar como tema transversal de governança digital (United Nations, 2013; United Nations, 2014). Essa institucionalização, entretanto, ocorre em paralelo a uma intensificação de arranjos securitários, observando-se o fortalecimento de regimes de compartilhamento de inteligência no âmbito da OTAN e, sobretudo, no interior da aliança Five Eyes, que continuou a expandir sua capacidade de interceptação global sob a justificativa de combate ao terrorismo e à criminalidade transnacional (Lyon, 2018). O caso paradigmático foi a aprovação, no Reino Unido, do *Investigatory Powers Act* (2016), frequentemente chamado de *"Snooper's Charter*", que consolidou poderes de vigilância em massa, inclusive para coleta de dados de navegação e armazenamento de metadados por provedores de serviços. Embora submetido a revisões judiciais e contestado por organizações da sociedade civil, o dispositivo britânico inspirou legislações semelhantes em países do Commonwealth e serviu de parâmetro para debates legislativos em democracias liberais consolidadas, demonstrando como as revelações de Snowden não produziram apenas retração, mas também legitimação de novos marcos normativos de vigilância (Wood, 2013; Kerr, 2017).

A pandemia de COVID-19 aparece, em certo sentido, como o catalisador mais recente de uma inflexão significativa no debate sobre vigilância, privacidade e governança digital, trazendo à tona mecanismos de monitoramento populacional que foram rapidamente legitimados sob a justificativa da emergência sanitária. Relatórios[3] da Freedom House (2020) enfatizaram que a crise acelerou processos em curso de consolidação de poderes de vigilância, com risco de normalização de práticas excepcionais em democracias liberais e

[3]Freedom House. "The Pandemic's Digital Shadow". In: *Freedom on the Net 2020*. Washington, DC: Freedom House, 2020. Available at: https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow

regimes autoritários. Nesse sentido, a pandemia pode ser interpretada como um "laboratório global" de tecnologias de rastreamento, cujo legado ultrapassa o campo da saúde pública e se inscreve no repertório ampliado de práticas securitárias. Um dos exemplos mais visíveis foi a adoção massiva de aplicativos de rastreamento de contatos. Em países europeus, iniciativas como o *Corona-Warn-App* (Alemanha) e o *Immuni* (Itália) foram apresentadas como voluntárias, baseadas em princípios de minimização de dados e descentralização, em conformidade com as diretrizes do Comitê Europeu de Proteção de Dados (EDPB, 2020). Em Singapura, o *TraceTogether* tornou-se, em pouco tempo, obrigatório para acesso a determinados espaços públicos, suscitando críticas quanto ao uso secundário de dados pelo Ministério da Saúde e pela polícia (CHOULIARAKI; STOLEROFF, 2021). Esses contrastes revelam a plasticidade do discurso da proteção de dados, que tanto pode servir como salvaguarda formal quanto como recurso de legitimação para práticas de controle intensificado.

No Oriente Médio, Israel se destacou como caso paradigmático. O governo autorizou a agência de segurança interna e contrainteligência, o Shin Bet, a utilizar dados de geolocalização coletados por operadoras de telecomunicações para rastrear deslocamentos de pessoas infectadas. Embora inicialmente concebida como medida temporária, a prática foi prorrogada diversas vezes, enfrentando questionamentos na Suprema Corte israelense, que advertiu para os riscos de consolidação de um regime de vigilância permanente, ilustrando como emergências podem ser mobilizadas para expandir prerrogativas de segurança já existentes, adquirindo status de normalidade[4]. Na América Latina, experiências diversas também receberam destaque - no Chile, o governo implementou sistemas de rastreamento georreferenciado, integrando informações de deslocamento com bancos de dados de saúde; na Argentina, aplicativos como o *Cuidar* foram exigidos para circulação em espaços públicos, incluindo a exigência de autodeclaração de sintomas e registros de mobilidade; e no Brasil[5], estados como São Paulo desenvolveram parcerias com operadoras de telecomunicações para criar o Sistema de Monitoramento Inteligente (SIMI), que permitia estimar taxas de isolamento social a partir de dados de telefonia móvel (Internetlab, 2020). Embora tais iniciativas tenham sido apresentadas como agregadas e anônimas, críticas apontaram a

[4] THE TIMES OF ISRAEL. *Suprema Corte limita a vigilância do Shin Bet sobre o coronavírus apenas àqueles que não cooperarem.* Israel: The Times of Israel, 1 mar. 2021. Disponível em: https://www.timesofisrael.com/high-court-limits-shin-bet-coronavirus-surveillance-to-those-wont-cooperate/

[5]INTERNETLAB. Proteção à privacidade nas medidas tecnológicas e alternativas adotadas no combate à Covid-19 no Brasil. São Paulo: InternetLab, 30 abr. 2021. Disponível em: https://internetlab.org.br/pt/noticias/privacy-and-data-protection-in-the-pandemic/

fragilidade dos mecanismos de auditoria independente e a ausência de garantias claras quanto ao descarte ou reaproveitamento posterior dessas bases de dados. Nesse contexto geral, o Relator Especial da ONU para o direito à privacidade advertiu em relatório de 2021 que medidas de vigilância sanitária deveriam observar critérios estritos de necessidade, proporcionalidade e limitação temporal, sublinhando que "medidas emergenciais não devem se converter em mecanismos permanentes de monitoramento social" (UNITED NATIONS, 2021). A advertência respondia ao fato de que diversos países utilizaram a pandemia para expandir programas de vigilância biométrica e de monitoramento de fronteiras, sob o argumento de contenção da propagação viral. A Electronic Frontier Foundation[6] (EFF, 2020), na mesma direção, denunciou casos em que tecnologias inicialmente justificadas pelo rastreamento de contatos foram integradas a programas policiais, inclusive em cidades norte-americanas, onde dados de mobilidade passaram a ser compartilhados com autoridades de segurança.

Ao mesmo tempo, a pandemia consolidava a inserção de empresas privadas no ecossistema da vigilância sanitária. A Apple e a Google, por exemplo, desenvolveram conjuntamente protocolos de rastreamento via *bluetooth*, foram incorporados por dezenas de países. Embora apresentados como compatíveis com princípios de minimização e consentimento, esses sistemas reforçaram a centralidade das grandes plataformas digitais como mediadoras de infraestruturas críticas, ampliando o debate sobre a privatização da governança da saúde e da vigilância (FELDSTEIN, 2019). Nesse mesmo período, empresas como a *Palantir* expandiram contratos com governos europeus e latino-americanos para oferecer soluções de integração e análise de dados, revelando como a emergência sanitária abriu novos mercados de "segurança da informação em saúde" (VELKOVSKA, 2022). Nessa perspectiva, a COVID-19 reforçou a ambivalência entre proteção e controle, na medida em que práticas de vigilância foram normalizadas como parte de um repertório de "cuidados" coletivos, ao mesmo tempo em que se consolidaram arranjos de responsabilização individual e coletivas digitais de rastreabilidade. (Lyon, 2021.)

A reconstrução empreendida no Capítulo 1 permitiu situar a vigilância como prática constitutiva da ordem política internacional contemporânea. Da Guerra Fria ao 11 de setembro, do PRISM às tecnologias pandêmicas, procuramos evidenciar que a racionalidade

[6]Electronic Frontier Foundation. *COVID-19 and Digital Rights.* San Francisco: Electronic Frontier Foundation, 2021. Disponível em: https://www.eff.org/issues/covid-19

da segurança se expandiu por meio de redes transnacionais, nas quais infraestruturas técnicas, interesses corporativos e aparatos estatais se entrelaçam. Esse percurso sugere que a vigilância não pode ser compreendida como um fenômeno contingente ou episódico, mas como tecnologia de governo que atravessa fronteiras e funda novas condições de legibilidade e intervenção sobre populações. É a partir desse pano de fundo que se torna possível compreender como a privacidade emergiu como categoria central no plano internacional. Não mais uma noção ligada à esfera individual ou a proteções constitucionais internas, mas uma linguagem jurídica e política mobilizada em foros multilaterais, em regimes regulatórios e em arranjos normativos capazes de projetar efeitos extraterritoriais.

2. Arquiteturas institucionais da vigilância para uma economia política da privacidade

Cyberspace.
A consensual hallucination experienced daily by billions
of legitimate operators, in every nation.

William Gibson, *Neuromancer* (1984)

No presente capítulo pretendemos identificar alguns dos paradoxos constitutivos do capitalismo neoliberal-digital, no qual a liberdade informacional se torna inseparável da vigilância e da modulação, e a regulação da privacidade contribui, por vezes, para a legitimação de sua própria erosão (Cohen, 2013; Zuboff, 2019; Browne, 2015; Rouvroy, 2016), conforme procuraremos desenvolver. A hipótese central que orienta esta tese é a de que a privacidade contemporânea não pode ser compreendida fora de sua inscrição na lógica político-econômica do tempo presente – um sistema global assimétrico, operado por um punhado de empresas transnacionais e sustentado por um ecossistema de normas, contratos, APIs, protocolos e práticas regulatórias que produzem determinadas condições - subjetivas e objetivos - para a governança das relações internacionais-digitais.

Nesse cenário, pretendemos demonstrar que o que se convencionou chamar de proteção de dados opera frequentemente como um dispositivo legitimador da exploração preditiva da experiência humana, normalizando práticas de modulação comportamental e antecipação mercadológica sob o signo da legalidade e do consentimento informado (Zuboff, 2019; Rouvroy e Berns, 2013; Mejias e Couldry, 2019), erguidas em torno dos pressupostos centrais das mutações contemporâneas da produção, sobretudo na forma do chamado capitalismo de vigilância (Zuboff, 2019).

Mais do que a simples mercantilização da informação, como veremos, trata-se de uma reorganização do espaço social e subjetivo, por meio da qual as interações digitais, hábitos de consumo e preferências pessoais passam a ser convertidas em ativos econômicos e ferramentas de normalização das relações sociais. A ascensão das plataformas digitais como atores político-econômicos-chave de nosso tempo desempenha papel central nesse processo, ao estruturar uma arquitetura sociotécnica na qual o comportamento dos usuários não só gera conteúdo, mas fundamentalmente retroalimenta fluxos de valor. No contexto das referidas transformações, a racionalidade neoliberal convocará, também, os indivíduos a assumirem a

responsabilidade por sua própria segurança, produtividade e exposição ao risco, como veremos na seção 2.2. A economia digital, assim como outros campos da vida social, passa a ser atravessada por lógicas de competição, desempenho e auto-investimento, articulando governamentalidade e subjetividade na paisagem tecno-informacional contemporânea.

Este capítulo, portanto, busca situar o capitalismo de vigilância no horizonte mais amplo de seu tempo, examinando sua emergência, fundamentos e implicações. A intenção não é abordar todos os elementos de forma exaustiva desde o início, mas fornecer uma base conceitual para compreender a relação entre a circulação dos dados, o Estado e o Mercado, abrindo caminho para nossa reflexão acerca da forma particular assumida pela agenda política da privacidade no século XXI.

2.1 Instituições, interpretações e mercados de dados: alguns alicerces do capitalismo da vigilância

A noção de capitalismo de vigilância, desenvolvida sobretudo por Shoshana Zuboff em *The Age of Surveillance Capitalism* (2019), descreve uma nova mutação do capitalismo contemporâneo em que a extração, análise e monetização de dados pessoais se tornam a lógica de acumulação primordial de nosso tempo. Trata-se de um regime em que os comportamentos humanos capturados por meio de rastros digitais, interações em plataformas, geolocalização, consumo e estados afetivos, são transformados em matéria-prima para a produção de mercadorias preditivas. O diferencial, em relação a formas anteriores de capitalismo, não reside exclusivamente na mercantilização da informação, mas também no fato de que a vida cotidiana é incorporada em sua integralidade como recurso econômico, colonizando o espaço íntimo e subjetivo:

> Não pode haver fronteiras que limitem a escala na caça por superávit comportamental nem território isento de ser saqueado. A afirmação dos direitos de escolha sobre a expropriação da experiência humana, sua conversão em dados e os usos destes são efeitos colaterais do processo, inseparáveis como a sombra de um objeto. Isso explica por que as cadeias de suprimento do Google começaram com a busca, mas se expandiram constante e regularmente para abranger novos e ainda mais ambiciosos territórios, longe de cliques e consultas. Os depósitos de superávit comportamental do Google agora abarcam tudo que faz parte do meio on-line: buscas, e-mails, textos, fotos, canções, mensagens, vídeos, localizações, padrões de comunicação, atitudes, preferências, interesses, rostos, emoções, doenças, redes sociais, compras e assim por diante. Um novo continente de superávit comportamental é confeccionado a cada instante a partir dos muitos fios virtuais da nossa

> vida cotidiana quando elas colidem com o Google, o Facebook e, de forma mais geral, com qualquer aspecto da arquitetura mediada por um computador com acesso à internet. De fato, sob a direção do capitalismo de vigilância, o alcance global da mediação pelo computador é redefinido como uma arquitetura de extração. (ZUBOFF, 2019, p. 343)

Em torno deste conjunto de categorias, o coletivo Tiqqun propõe uma chave analítica complexa para pensar as transformações contemporâneas da produção de valor, principalmente levando em consideração o avanço da informatização entre as décadas de 1930 e 1970. Implicando no refinamento e descentralização das técnicas de equilíbrio entre oferta e demanda típicas da metáfora da "mão invisível" do mercado, que passa a ser inscrita nas funções das tecnologias computo-informacionais, nota-se a progressiva automatização de intermediações mercantis e financeiras, além do mapeamento e indução de preferências de consumo (TIQQUN, 2015), sobre o qual se debruçará Zuboff. A informação sobre o comportamento dos agentes econômicos se converte, nesse cenário, em um ativo que circula nos mercados em forma de títulos financeiros, de modo que cada sujeito da valorização capitalista se torna um *feedback* em tempo real. De um lado, consolida-se a percepção da informação como fator produtivo autônomo, distinto do trabalho e do capital, mas igualmente decisivo para o crescimento econômico; de outro, um setor inteiro dedicado à produção e acumulação de informações. Essa dupla dinâmica sustenta o que se convencionou chamar de economia da informação, onde a informação torna-se a riqueza a ser explorada e acumulada, transformando o capitalismo em auxiliar da cibernética e, por consequência lógica, sediando o terreno para sua versão contemporânea sob título de capitalismo da vigilância.

Se depois de 1929 o aparato estatístico visava à regulação macroeconômica, após 1973, sugere Tiqqun, a própria regulação social passa a se apoiar na valorização informacional. A *Hipótese Cibernética* (2015), nesse sentido, propõe que o capitalismo já não pode ser compreendido como um sistema de acumulação de mercadorias, trata-se de uma engrenagem auxiliar de um aparato global de comunicação e controle (ou seja, a cibernética propriamente dita). Trata-se de uma transformação que não se explica pela substituição do regime industrial pelo regime financeiro-informacional, tampouco pela alteração no estatuto do trabalho, mas sim pelo deslocamento mais profundo da centralidade das mercadorias e dos indivíduos para a informação digital, operada como meio de segurança, vigilância e modulação das condutas.

Não se trata de coordenar indivíduos e mercadorias, mas efetivamente de instituir um sistema comunicacional de controle universal, onde tudo é potencialmente apreensível, codificável e previsível. De acordo com seu princípio fundamental, todos os seres — vivos, técnicos, materiais ou sociais — emitem, recebem e processam informações passíveis de controle, desde que submetidas ao programa adequado. O projeto cibernético, sintetiza Rodriguez (2015) *"visava libertar a comunicação das limitações humanas, transformando-a em processo maquínico e vivo, antecipando assim as biotecnologias e inaugurando um campo em que vigilância e segurança se confundem com a própria lógica da vida"* (RODRIGUEZ, 2015, p. 13). O projeto ao qual Tiqqun faz referência não permanece no plano teórico ou filosófico, tendo suas premissas sobre comunicação como processo universalmente codificável e controlável se concretizado na engenharia de redes digitais desde a segunda metade do século XX. A lógica de fragmentação, roteamento e interoperabilidade, nesse sentido, nada mais é do que a aplicação prática do princípio cibernético de que fluxos de informação podem ser modulados, monitorados e estruturados para otimizar previsibilidade e resiliência. A materialização deste processo pode ser observada na própria gênese da Internet, que emerge como um território livre da coordenação humana, inaugurando protocolos, arquiteturas e dispositivos capazes de operacionalizar a visão de controle abrangente delineada pelos teóricos da ciência cibernética.

Nos Estados Unidos, a Rede da Agência para Projetos de Pesquisa Avançada (do inglês, *Advanced Research Project Agency Network*, ou ARPA), vinculada ao Departamento de Defesa, liderou a criação da ARPANET, protótipo original da futura rede global. Um de seus importantes alicerces técnicos foi a formulação de Paul Baran sobre o *packet switching*, técnica que transformou a lógica das comunicações ao permitir que mensagens fossem fragmentadas em pacotes independentes e roteadas por caminhos múltiplos, explorando a redundância e a flexibilidade das redes digitais (ABBATE, 1999; KOSTECZKA, 2024). À luz da hipótese cibernética de Tiqqun, essa arquitetura distribuída antecipava uma lógica de circulação, registro e governança dos fluxos, configurando uma infraestrutura capaz de organizar, modular e quantificar comportamentos sociais de forma invisível, ainda que originalmente voltada a fins militares. Embora inspirado na telefonia e no telégrafo, o *packet switching* se diferenciava pela granularidade do digital, capaz de converter sinais em sequências discretas de números binários. Cada pacote, munido de endereço e instruções, podia trafegar por rotas autônomas até a recomposição da mensagem no destino. Essa

concepção, desenvolvida na RAND Corporation[7] sob demanda militar, buscava um sistema resiliente e descentralizado, apto a sobreviver a ataques que pudessem porventura neutralizar sistemas analógicos de comunicação. Nesse contexto, a ARPANET não foi apenas uma inovação técnica (ABBATE, 1999), mas a materialização de uma estratégia política e militar em plena Guerra Fria, quando a comunicação distribuída representava uma forma de defesa diante de um inimigo concebido como imprevisível. Ao mesmo tempo, engenheiros da ARPA, como Lawrence Roberts e Leonard Kleinrock, enfrentavam desafios de interoperabilidade entre computadores heterogêneos, abrindo caminho para o desenvolvimento de protocolos de comunicação, embriões do TCP/IP[8]. Esses esforços coletivos revelam também o caráter normativo da infraestrutura digital, que, posteriormente, evidencia a transição de um projeto militar para um ecossistema civil e, mais tarde, comercial. A introdução da Ethernet[9] por Robert Metcalfe, a formulação da lei do "efeito de rede"[10] e a criação do TCP/IP exemplificam esse deslocamento, no qual a lógica da conexão constante passou a fundamentar os modelos de negócios das grandes plataformas digitais.

Mesmo o imaginário utópico da cibercultura e da ciberdemocracia, que emergiu nos anos 1990 com promessas de liberdade, participação horizontal e democratização do acesso à informação, encontrou limites concretos na própria infraestrutura técnica da rede. Protocolos como TCP/IP, padrões como a Ethernet e o crescimento exponencial dos usuários revelaram

[7] A Research and Development Corporation é um think tank estadunidense, fundado em 1948, a princípio com o objetivo de desenvolver pesquisa e análise estratégica para o Departamento de Defesa dos Estados Unidos. Seu objetivo principal era aplicar métodos quantitativos e modelos científicos para problemas complexos de política militar e tecnológica, incluindo logística e operações militares.

[8] O TCP/IP é o conjunto de protocolos de comunicação que define como os dados são transmitidos, roteados e recebidos em redes digitais, incluindo a Internet. Derivado de dois protocolos centrais, o TCP (Transmission Control Protocol), que garante que os dados enviados sejam entregues de forma integral e ordenada, fragmentando informações em pacotes e reconstituindo-os no destino mesmo que cheguem fora de ordem ou por caminhos diferentes, e o IP (Internet Protocol), responsável pelo endereçamento e roteamento dos pacotes, determinando os caminhos que cada um deve seguir até alcançar o destino correto. O TCP/IP funciona em um modelo em camadas, separando as funções de transporte, rede, aplicação e link físico, e foi projetado para conectar redes heterogêneas, permitindo que computadores distintos se comuniquem independentemente do hardware ou sistema operacional. Sua escalabilidade e flexibilidade fizeram dele a base da Internet moderna, a partir da padronização nos anos 1980, substituindo protocolos anteriores da ARPANET e possibilitando a expansão global da rede.

[9] A Ethernet é uma tecnologia de rede local que define padrões para a transmissão de dados entre computadores e dispositivos em uma mesma rede física. Criada por Robert Metcalfe nos anos 1970, a Ethernet especifica tanto o meio físico (como cabos de cobre ou fibras ópticas) quanto os protocolos de comunicação que permitem que pacotes de dados sejam enviados, detectando e gerenciando colisões de informações no meio compartilhado. Originalmente, a Ethernet fazia uso de um método de acesso chamado CSMA/CD (Carrier Sense Multiple Access with Collision Detection), que permitia que múltiplos dispositivos compartilhassem o mesmo canal de comunicação de forma organizada, evitando perdas de dados. Com o tempo, a tecnologia evoluiu para versões mais rápidas e seguras, incluindo redes comutadas (switches) e conexões de alta velocidade, tornando-se o padrão dominante para redes locais em empresas, instituições e residências.

[10] A lei do efeito de rede descreve o fenômeno em que o valor de um produto ou serviço aumenta à medida que mais pessoas o utilizam. No contexto da Internet, explica por que tecnologias como o TCP/IP e a Ethernet se tornaram padrões dominantes: quanto mais computadores e instituições adotavam esses protocolos, maior sua utilidade e influência, consolidando a infraestrutura global e pavimentando o caminho para a lógica de negócios das grandes plataformas digitais.

que a liberdade prometida dependia de sistemas complexos, projetados originalmente para fins militares ou corporativos, que estruturavam e controlavam a circulação de dados de forma substantiva. Ao mesmo tempo, essas utopias foram rapidamente moduladas pelas forças econômicas que sustentavam e exploravam a Internet, na forma da mercantilização dos fluxos de informação e da centralização gradual em grandes plataformas digitais que passaram a condicionar quais usos eram viáveis, quais comportamentos eram incentivados e qual forma de participação era aceitável. A promessa tecno-otimista de um espaço de profunda horizontalidade se mostrou, portanto, sempre tensionada por limites técnicos, estratégicos e econômicos, antecipando as contribuições de Zuboff quanto à governança dos fluxos computo-informacionais. Integrando a hipótese cibernética, a Internet emerge como um espaço de captura, subjetivação e governança invisível, no qual protocolos, algoritmos e fluxos de informação consolidam uma trama de interesses estratégicos, disputas por padronização e reconfigurações políticas que estruturaram a rede até a privatização e a hegemonia das plataformas (TURNER, 2006), preparando o terreno para a concepção do capitalismo de vigilância apresentada pela autora.

Do ponto de vista analítico, portanto, o capitalismo de vigilância não se restringe à exploração passiva de dados, ao passo que introduz um ciclo de retroalimentação comportamental, no qual algoritmos e sistemas de inteligência artificial preveem e progressivamente condicionam e orientam condutas, reduzindo contingências e maximizando a previsibilidade. Esse movimento implica em uma transição de uma economia baseada na produção de bens e serviços para uma economia de captura e predição de comportamento, consolidando o deslocamento para a técnica difusa da governamentalidade algorítmica (ROUVROY, 2015), modelando possibilidades de presente e futuro.

Em geral, a literatura que procurou se debruçar sobre esse fenômeno localizará, justamente, no aparente fracasso da Web 1.0 - fundamentalmente estática e de reduzidas possibilidades de produção de conteúdo rentável - e na subsequente conversão da Google em uma das maiores corporações do mundo a emergência de novas estratégias para resgatar a confiança na indústria “ponto-com”, no contexto imediatamente posterior ao estouro da bolha da internet (FUCHS, 2017).

É diante da necessidade de reconquistar investidores que passa a ser rapidamente difundida a noção de que os anos 2000 estariam em face de uma nova experiência de grande

potencial inovador - seja do ponto de vista econômico, seja do ponto de vista de sua natureza supostamente horizontal e participativa. A partir da literatura que buscou analisar criticamente as categorias que acompanharam a ascensão da Web 2.0 (FUCHS, 2017; CARPENTIER e DeCLEEN, 2008; VAN DIJCK, 2009; TERRANOVA, 2004), partimos da constatação de que o termo "participação" não é unívoco, mas múltiplo e disputado principalmente em termos de sua mobilização em relação a Internet no século XXI, quando com frequência passa-se a assumir todos os usuários como automaticamente "co-produtores" ou "criadores de conteúdo", independentemente de sua ação restrita na forma da reação e da circulação de conteúdo, sem, efetivamente, tocar nas estruturas de poder ou produção atravessadas pelas "novas" mídias (CARPENTIER e De CLEEN, 2008) A aparência de abertura, nesse cenário, passa a conviver com profundas desigualdades de acesso, visibilidade e reconhecimento, ocultando a perspectiva de que poucos detêm efetivamente os meios e a autoridade para moldar esse ecossistema comunicacional.

Tiziana Terranova apostará na noção de *free labor* — ou "trabalho gratuito" — na cultura digital, em sua caracterização do contexto. Para a autora, a Web 2.0 não pode ser entendida em termos de um espaço de participação ou de criatividade descentralizada, mas um campo de exploração econômica, em que o tempo, a energia e a inventividade dos usuários são mobilizados sem remuneração direta, mas com gigantesco valor para as plataformas e corporações que estruturam a rede. Terranova argumenta que esse "trabalho gratuito" não é um desvio acidental, mas um elemento constitutivo do modelo da internet comercial e da lógica cultural do capitalismo informacional. A atividade dos usuários — ao postar, comentar, recomendar, classificar, remixar ou simplesmente ao navegar — gera dados e conteúdos, capturados e transformados em mercadorias, seja pela venda de publicidade direcionada, seja pela construção de bases de dados que alimentam processos de acumulação. A promessa de liberdade e participação que caracteriza o discurso da Web 2.0, portanto, convive com a extração sistemática de valor de práticas sociais não remuneradas, implicando em um território de convívio da exploração do trabalho gratuito e da expressão de desejo, criatividade e sensibilidade típicos da cultura digital. Nesse sentido, a autora antecipará debates que depois se consolidaram em torno de conceitos como *plataformização* - estruturante da Internet em sua forma contemporânea e relaciona à forma como as plataformas digitais operam na produção de infraestruturas definidoras de regras e formatos

de comunicação e, ao mesmo tempo, organizadoras do mercado e da esfera pública (VAN DIJCK, 2009)

O conceito de plataforma — muitas vezes usado de forma genérica e ambígua — pode ser observado em termos de seu duplo funcionamento como um marcador preciso e como um conceito vago (GILLESPIE, 2010), capaz de atravessar diferentes campos discursivos. José van Dijck, Thomas Poell e Martijn de Waal (2018) propõem defini-la como uma arquitetura digital programável, estruturada para organizar interações entre usuários, empresas e órgãos públicos, permitindo a coleta sistemática, o processamento algorítmico e a monetização de dados. Distinguindo entre os diferentes tipos de plataformas[11], os autores evidenciam uma dinâmica de expansão, aquisições e diversificação de modelos de negócios correlatos, evidenciando a fluidez dessas categorias e do próprio fenômeno da plataformização, no qual as corporações redesenham repetidamente as relações nas quais elas mesmas se inscrevem:

As diferentes perspectivas sobre plataformização sugerem que esse processo se desenrola em três dimensões institucionais: infraestruturas de dados, mercados e governança. E observamos que, a partir de uma perspectiva dos estudos culturais, a plataforma leva à (re)organização das práticas culturais em torno de plataformas, enquanto essas práticas moldam simultaneamente as dimensões institucionais de uma plataforma. Por fim, as atividades coletivas de usuários finais e complementadores e a resposta dos operadores das plataformas a essas atividades determinam o crescimento contínuo de uma plataforma ou o seu fim. Conforme apontado por pesquisadores da área de economia política crítica, as relações de poder entre operadores de plataforma, usuários finais e complementadores são extremamente voláteis e inerentemente assimétricas, uma vez que os operadores são totalmente responsáveis pelo desenvolvimento tecnoeconômico de uma plataforma.

> Os efeitos de rede, juntamente com estratégias das plataformas que frustram as tentativas dos usuários finais ou complementadores de sair de uma plataforma, têm resultado em mercados de plataformas altamente concentrados (BARWISE; WATKINS, 2018). Enquanto as indústrias midiáticas e de telecomunicações são dominadas por conglomerados que operam internacionalmente há décadas (WINSECK, 2008), o rápido surgimento de um punhado de empresas de plataformas desafia o poder dos operadores históricos dessas indústrias. Alguns exemplos pungentes do domínio digital por empresas de plataformas podem ser testemunhados nos novos mercados de publicidade digital, aplicativos,

[11] As infraestruturais, como Google, Apple, Facebook, Amazon e Microsoft, que formam o núcleo do ecossistema digital e atuam como gatekeepers do fluxo de dados; e as setoriais, como Uber, Airbnb ou iFood, que conectam usuários e prestadores de serviços sem necessariamente possuir ativos físicos ou funcionários próprios

> comércio eletrônico e computação em nuvem. Com essas considerações em mente, propomos estudar três dimensões institucionais da plataformização como processos interativos que envolvem uma ampla variedade de atores, mas que também são estruturados por relações de poder fundamentalmente desiguais. (POELL, NIEBORG E DIJCK, 2020, p. 5)

Zuboff (2019) tensionará, em certo sentido, as análises que priorizaram a noção de economias de plataforma (VAN DIJK, 2009; SRNICEK, 2017) ao enfatizar que a plataformização não se limita à organização de ecossistemas digitais nem à extração de valor econômico a partir de fluxos de dados, estando em jogo, de fato, a emergência de um novo regime de acumulação que se apoia na captura contínua da experiência humana (ZUBOFF, 2019). Mais do que plataformas mediadoras que moldam práticas sociais (VAN DIJCK, 2009), trata-se da conversão para uma lógica mais ampla de apropriação da vida cotidiana como matéria-prima para processos de predição e modulação de comportamentos. O que aparece como liberdade de participação é, para Zuboff, uma forma de sujeição invisível por meio da qual a atenção e a ação dos usuários se tornam variáveis ajustadas a partir de arquiteturas algorítmicas que buscam garantir eficiência, engajamento e consumo acima de tudo.

Particularmente preocupada com a relação entre o Estado e as *Big Techs*, Zuboff argumenta não se tratar de padrões de cooperação ou de regulação insuficiente, mas de uma convergência estrutural de interesses. Ou seja, o capitalismo de vigilância encontra terreno fértil para sua consolidação no contexto da primeira década dos 2000 justamente diante não apenas da aparente tolerância indiscriminada do Estado contemporâneo, mas com frequência por conta de sua dependência das práticas de captura e análise de dados conduzidas pelas corporações digitais. Nesse sentido, a autora sustenta que o Estado desempenha um papel ambíguo: de um lado, em nome da "soberania e da proteção de direitos", opera como um agente regulador da coleta e do uso de dados pessoais enquanto, do outro, as próprias agências estatais, em particular no campo da segurança nacional e da inteligência, encontram nas plataformas parceiros estratégicos para ampliar suas capacidades de vigilância. Essa lógica se intensifica no contexto posterior ao 11 de setembro, conforme discutido no Capítulo 1, contexto no qual a "guerra ao terror" abre um horizonte normativo e político favorável à expansão da coleta massiva de dados:

> Os ataques terroristas de 11 de Setembro empurraram a comunidade de inteligência na direção de uma curva de demanda desconhecida que

> insistia em aumentos exponenciais na velocidade. Como todo seu sigilo, mesmo a NSA se encontrava sujeita às questões de tempo e às restrições jurídicas de um Estado democrático. Os andamentos da democracia são, por definição, lentos e pesados por redundâncias, freios e contrapesos, leis e regras. As agências buscavam métodos de mobilização de equipe que pudessem ultrapassar com agilidade as restrições jurídicas e burocráticas. Nesse ambiente de trauma e ansiedade, um "estado de exceção" foi invocado para legitimar um novo imperativo: rapidez a qualquer custo (...) A missão do Google era organizar e tornar acessível a informação e no fim de 2001 a comunidade de inteligência estabeleceu o domínio da informação no ambiente público, logo institucionalizando-o em infraestrutura, funcionários e práticas de tecnologia global patrocinada pelo Estado representando centenas de bilhões de dólares. Os contornos de uma nova interdependência entre agentes públicos e privados de domínio da informação começaram a surgir, algo que é bem mais entendido se olharmos através daquilo que o sociólogo Max Weber certa vez chamou de "afinidade eletiva", nascida de um magnetismo mútuo que se origina em intenções, interesses e reciprocidades compartilhadas. (ZUBOFF, 2019, p. 179)

Para Zuboff, portanto, as plataformas ocupam, em meados dos 2000, um vazio regulatório potencializado pela ausência de políticas robustas de proteção de dados e privacidade nos Estados Unidos, recorrendo repetidamente à retórica da inovação e da liberdade de mercado para evitar controles públicos. O Estado neoliberal - conforme interpretação da autora - teria funcionado como condição de possibilidade para que as *Big Techs* expandissem suas práticas de extração de dados sem grandes resistências jurídicas ou políticas. Zuboff, entretanto, insiste que a relação entre Estado e plataformas representa um novo pacto de poder, que não pode ser entendido apenas como privatização ou terceirização de funções públicas, mas como uma verdadeira fusão de racionalidades no interior da qual o Estado ganha acesso a mecanismos de vigilância, enquanto as empresas consolidam seu poder econômico sob a legitimação implícita de políticas de segurança nacional e de ordem pública. A posição da autora, neste ponto, não é livre de desacordos. McChesney, por exemplo, enfatiza que o Estado neoliberal não teria um espectador passivo ou simplesmente conivente dessa transformação, mas um interventor ativo ao promover a desregulação dos setores de mídia e telecomunicações e criando condições jurídicas fundamentais para o livre desenvolvimento das *Big Tech* em seu máximo potencial de exploração:

> A explicação convencional sobre a comunicação globalizada costuma centrar-se na tecnologia: argumenta-se que os avanços radicais nas tecnologias de comunicação tornaram possíveis os fluxos midiáticos globais e as operações empresariais em escala mundial e que, em geral, tudo isso é algo positivo. No entanto, essa é uma interpretação enganosa. Por trás das novas tecnologias de comunicação existiu uma força política: a virada para a ortodoxia neoliberal, que afrouxou ou eliminou barreiras à

> exploração comercial da mídia, ao investimento estrangeiro em sistemas de comunicação e à concentração da propriedade midiática. Não há nada intrínseco à tecnologia que exigisse o neoliberalismo; as novas comunicações digitais poderiam, por exemplo, ter sido usadas simplesmente para aprimorar a oferta de serviços públicos, caso uma sociedade assim o tivesse escolhido. Entretanto, inseridas em um arcabouço de práticas e políticas neoliberais, as comunicações tornaram-se subitamente sujeitas a um desenvolvimento corporativo-comercial transnacional. A ascensão do neoliberalismo foi complexa, mas, sempre que possível, cuidadosamente orquestrada. O governo dos Estados Unidos, em particular, atuou de forma agressiva e persistente como se apenas um sistema midiático orientado pelo lucro — como o dos EUA, com seu modelo de jornalismo profissional — pudesse ser considerado aceitável em uma sociedade livre. Como muitas nações não atendiam a esse padrão, o governo norte-americano empenhou-se em eliminar barreiras para que os povos do mundo tivessem maior exposição, se não à mídia baseada nos EUA, ao menos a um modelo comercial de mídia no estilo norte-americano. Após a desregulamentação nacional da mídia em países centrais como os Estados Unidos e o Reino Unido, seguiram-se medidas de alcance transnacional, como o Acordo de Livre Comércio da América do Norte (NAFTA) e a Organização Mundial do Comércio (OMC), ambas voltadas à criação de mercados regionais e globais (Mosco e Schiller, 2001). Por outro lado, os Estados Unidos abriram seletivamente parcelas significativas de seu incomparável mercado interno de mídia — sobretudo nos setores de cinema, gravação e publicação —, estendendo de forma mais limitada essa abertura à radiodifusão e às telecomunicações, para permitir um investimento corporativo estrangeiro cada vez mais amplo. (McCHESNEY e SCHILLER, 2003, p. 7. Tradução nossa.)

Em direção complementar, Evgeny Morozov (2013) tensiona de modo significativo a interpretação de Zuboff sobre a convergência de interesses entre Estados e plataformas, propondo uma inflexão crítica na forma de uma engenharia política deliberada, incompatível em certo sentido com a ênfase nos vácuos regulatórios localizados por Zuboff. Tendo também denunciado (2011) a ilusão da Internet como um espaço de participação e liberdade, Morozov descreve um ambiente infraestrutural determinado por interesses geopolíticos norte-americanos, constituindo uma narrativa ideológica dissimulada da expansão estratégica das plataformas e de práticas de vigilância globais. Nesse enquadramento, as *startups* do Vale do Silício se reinventam diante da crise dos anos 2000 como extensões de um ecossistema marcado por alianças constitutivas entre a academia, o Estado e as forças armadas (Morozov, 2011) responsável pela própria configuração da arquitetura das redes contemporâneas. Esse complexo industrial-militar-digital-estatal-acadêmico - em diálogo com McChesney (2013) - teria posicionado empresas como Google, Microsoft e Amazon como ativos estratégicos da política externa norte-americana, materializados por exemplo em contratos de nuvem para a CIA e o Departamento de Defesa, exemplos de como a fronteira entre interesses estatais e

corporativos é borrada de forma estrutural, e não contingente, como parece por vezes supor a tese da autora.

A "não regulação" aparece, assim, como política de Estado voltada a garantir superioridade tecnológica dos Estados Unidos no cenário internacional, reconfigurando assimetrias globais (Morozov, 2013). Ao contrário de Zuboff, cuja crítica se concentra no imperativo de impor limites regulatórios a um capitalismo de vigilância que teria crescido à revelia do Estado, Morozov desloca a questão para o campo da produção intencional de mercados digitais no interior do Estado neoliberal, arquiteto *ativo* das condições que possibilitaram a plataformização da economia global.

A dimensão geopolítica não é inteiramente esquecida por Zuboff, evidentemente, compreendendo a especificidade da inserção das *Big Tech* como uma que se traduz de forma transnacional, contornando regulamentações nacionais e maximizando sua liberdade operacional a partir de jurisdições múltiplas. Contratos públicos, acordos de inteligência, programas de segurança e serviços administrativos seriam frequentemente mediados ou viabilizados por plataformas privadas, ao redor do planeta. Essa articulação contribuiria para delegar funções regulatórias e de monitoramento a corporações transnacionais, implicando no controle direto sobre fluxos de informação e dados sensíveis, representando uma possibilidade sem precedentes de governança indireta nas mãos das plataformas digitais, principalmente por meio do que Zuboff chamará de "poder instrumentário", típico do contexto da ascensão do capitalismo da vigilância:

> O totalitarismo atuava por intermédio da violência, mas o poder instrumentário opera através da modificação comportamental, e é aí que o nosso foco precisa mudar. O poder instrumentário não tem interesse nas almas nem tem qualquer princípio a instruir. Não há qualquer treinamento ou transformação para a salvação espiritual, qualquer ideologia pela qual julgar nossas ações. Ele não exige a possessão de cada pessoa de dentro para fora. Ele não tem interesse em exterminar nem desfigurar nossos corpos e mentes em nome da devoção pura. (...) Ele não tem apetite pelo nosso sofrimento, dor ou terror, embora receba com avidez e de bom grado o superávit comportamental que é filtrado a partir de nossa angústia. Treinado em ação mensurável, ele só se preocupa com que tudo feito por nós seja acessível a suas operações, em constante evolução, de renderização, cálculo, modificação, monetização e controle. (...) O totalitarismo era um projeto político que convergia com a economia para dominar a sociedade. O instrumentarianismo é um projeto de mercado que converge com o digital para alcançar seu próprio e exclusivo tipo de dominação social. (ZUBOFF, 2019, p. 700)

Caracterizado, portanto, por uma forma de dominação que não se ancora na violência física ou em mecanismos clássicos de coerção política, o "poder instrumentário" se sustenta pela captura invisível de dados e na manipulação remota de condutas. Ele prescinde do terror de Estado, do fechamento de instituições democráticas ou da perseguição aberta. Ao contrário, avança por meio de técnicas discretas de auto-autorização corporativa, pelo uso de eufemismos que ocultam sua lógica extrativa e por estratégias retóricas que confundem a percepção pública acerca de sua extensão, na forma de uma tecnologia de poder que se expande reorganizando os parâmetros de escolha individual e de interação coletiva sem declarar diretamente seu propósito (Zuboff, 2019), incorporando o comportamento humano em sistemas algorítmicos de previsão e modulação[12]. A experiência cotidiana é, então, convertida em "excedente comportamental", transformado em ativo econômico, dissolvendo gradualmente a autonomia individual em um ambiente de orientação de preferências e decisões em consonância com interesses e prioridades das plataformas. Assim, o poder instrumentário implica numa forma de governamentalidade que age à distância, desloca-se sorrateiramente, cria certezas técnicas que naturalizam a exploração e, sobretudo, esvazia a noção de liberdade como autodeterminação (Zuboff, 2019). Sua força não está no choque, mas na normalização de práticas que convertem participação cultural em participação produtiva e, por fim, em matéria-prima de vigilância e intervenção comportamental.

À luz do "poder instrumental" Zuboff articula dois imperativos centrais do capitalismo de vigilância: o imperativo da extração e o imperativo da predição. O primeiro se refere à coleta contínua e sistemática de dados comportamentais, enquanto o segundo ultrapassa a esfera da antecipação, avançando para a modulação comportamento por meio de intervenções algorítmicas. Notificações temporizadas, ajustes de feeds, sugestões direcionadas e até manipulação de objetos físicos — como travas em automóveis ou temporização de botões de compra — exemplificam como as plataformas passam a operar

[12] Embora semelhanças sejam evidentes entre o "poder instrumentário" em Zuboff e a "governamentalidade algorítmica" em Rouvroy, ressaltamos que se tratam de conceitos distintos, em sua essência. O conceito de poder instrumentário refere-se a uma forma de dominação própria do capitalismo de vigilância, em que os dados pessoais são capturados, processados e transformados em instrumentos de previsão e modulação do comportamento, operando de maneira extrajurídica e extra institucional, apoiado principalmente em infraestruturas digitais privadas, com vistas à mercantilização da experiência humana e ao controle orientado ao lucro. Já a noção de "governamentalidade algorítmica" desloca o foco para os modos de condução das condutas mediados por sistemas algorítmicos que não apenas predizem, mas estruturam possibilidades de ação. Enquanto o poder instrumentário se ancora na lógica econômica de extração e comercialização de dados, a governamentalidade algorítmica enfatiza a dimensão biopolítica dos algoritmos como dispositivos que regulam populações, normatizam comportamentos e produzem realidades sociais, operando numa camada de governo difusa, preventiva e probabilística.

sobre a conduta humana de maneira indireta, mas estruturante, convertendo a experiência em insumo econômico, alimentando um ciclo de acumulação que se sustenta na transformação contínua da vida social em dados extraíveis e monetizáveis. Ao recorrer à análise de Karl Polanyi sobre mercadorias fictícias, a autora insere o capitalismo de vigilância em uma tradição crítica que identifica a expropriação como elemento constitutivo da dinâmica capitalista. Tal como terra, trabalho e dinheiro foram artificialmente convertidos em mercadorias, a experiência humana, transformada em comportamento digital, configura uma "quarta mercadoria fictícia", cuja exploração é simultaneamente econômica, social e política.

É importante, nesse sentido, ressaltar que Zuboff (2019) localiza o capitalismo de vigilância como uma manifestação direta de objetivos econômicos, cuja expansão só se torna viável em um cenário de políticas neoliberais. Para a autora, esse modelo se fundamenta em uma tradição intelectual que legitima a centralidade do indivíduo empreendedor, representada por figuras como Friedrich Hayek e Milton Friedman, cujas ideias sustentam a noção de que o sucesso empresarial é um mérito exclusivamente pessoal, dissociado de qualquer rede coletiva ou institucional. Esse culto ao empreendedorismo destemido reforça a primazia da iniciativa privada, naturalizando a competitividade individual como princípio regulador das relações sociais e econômicas. Nesse contexto, Zuboff enfatiza que compreender o capitalismo de vigilância exige uma análise do neoliberalismo que ultrapasse sua dimensão restrita a políticas econômicas ou à atuação de instituições estatais e mercadológicas. O neoliberalismo deve, assim, ser analisado na forma de um dispositivo abrangente de reorganização social no qual a subjetividade individual e os fluxos de experiência coletiva são incorporados a circuitos econômicos e tecnológicos, articulados à lógica de expansão da mercantilização e da centralidade do capital sobre a vida social.

Sobre o paradigma neoliberal em torno do qual se desdobra a economia política da vigilância - e, por consequência, da privacidade em tempos de vigilância - nos voltaremos na próxima seção.

2.2 Do Estado ao Mercado, o paradigma neoliberal das sociedades da vigilância

O deslocamento que marca a ascensão do neoliberalismo não pode ser reduzido a um simples "recuo do Estado". Como demonstram Wendy Brown (2015) e Dardot e Laval (2016), o neoliberalismo opera sobretudo como racionalidade política abrangente, que reorganiza a própria forma de governo ao inscrever a lógica concorrencial em todas as esferas

da vida. Essa dimensão se articula intimamente com o cenário que procuramos desenhar na seção anterior, observando que a noção de racionalidade concorrencial se traduz, aqui, em dispositivos de coleta e análise de dados que modulam riscos, reputações e comportamentos em tempo real, evidenciando como a economia política neoliberal se faz inseparável de uma ecologia de vigilância distribuída.

A governamentalidade neoliberal aparece, no *Nascimento da Biopolítica* (2008b), traduzida em termos da reorganização do Estado e da sociedade a partir da lógica da concorrência e, para o que aqui nos é concernente, a assimilação por parte do indivíduo da responsabilidade sobre a gestão do "paradoxo" liberdade-segurança. O sujeito neoliberal é, portanto, aquele que assume para si os riscos de sua existência, que se previne, que *consome* segurança como um bem privado. Moldada por paradigmas adaptacionistas da biologia evolutiva (Stiegler, 2018), a biopolítica neoliberal teria assumido a sobrevivência como uma tarefa individual que depende da capacidade do sujeito de se *adaptar* - um novo imperativo político primordial - a ambientes em evolução constante e imprevisível. Trata-se, portanto, de uma função moral do indivíduo em lidar de forma plástica e flexível com os acontecimentos de seu ambiente social, econômico - e, no limite, digital. Essa virada, ao mesmo tempo, passa também a constituir o risco em estímulo permanente para manter o indivíduo competitivo (Stiegler, 2018). Como temos visto, é no interior deste processo que se abre o caminho, progressivamente, para formas de governo baseadas em algoritmos, na forma de um deslocamento decisivo: do governo dos corpos para o governo dos dados, erguido sobre a incerteza modelada por dispositivos computo-informacionais, revelando, no limite, uma transformação (infra)estrutural da segurança como tecnologia de governo.

Contemporaneamente, uma série de abordagens têm se dedicado a expandir e atualizar a contribuição foucaultiana no contexto da chamada racionalidade neoliberal, em geral tendo em comum a perspectiva de que o dispositivo de segurança adquiriu novas funções e formas coerentes com a produção de sujeitos empreendedores de si (Lemke, 2011; Stiegler,2018), sugerindo (Brown, 2015; Dardot e Laval, 2016) mostram como, nesse processo, o mercado deixa de ser espaço de trocas para se tornar norma de conduta, projetando a empresa como modelo universal de subjetivação. Assim, o *homo oeconomicus* contemporâneo é convocado a gerir a si mesmo como capital, submetido a métricas de desempenho, comparabilidade e eficiência. É nesse sentido que Dardot e Laval (2016) descrevem o neoliberalismo como um "novo racionalismo normativo", no qual a empresa é convertida em paradigma organizador

da vida social, materializando em termos de nosso debate o processo que Brown (2015) denomina "desdemocratização" na forma da erosão das instâncias públicas de decisão, pela naturalização de sistemas de monitoramento e predição que transformam direitos em variáveis de gestão. Fernanda Bruno (2013) ilumina essa articulação ao mostrar como práticas algorítmicas de coleta e predição funcionam como "máquinas de ver", (re)produtoras de sujeitos probabilísticos, compelidos a gerir riscos em termos de unidades comparáveis entre si (Dardot e Laval, 2016).

Lemke (2019) e Dean (2010) oferecem leituras complementares ao mostrar como esse regime desloca a ênfase das instituições para a autogestão individual, instaurando uma economia moral do risco em que a insegurança é normalizada como condição de liberdade. Esse cenário se traduz em termos da internalização normativa da vigilância (Lemke, 2019), interpelando sujeitos (em nosso caso, de dados) por métricas, índices e auditorias, num ambiente onde segurança significa projetar e otimizar a si mesmo - senão principalmente - diante de cenários incertos. Bruno (2013) reforça essa perspectiva ao mostrar que a subjetividade neoliberal se constitui pela interação constante com dispositivos de avaliação e rastreamento, que convertem condutas em dados monetizáveis.

Brown sintetiza:

> A atual economicização neoliberal da vida política e social se distingue por uma produção discursiva que converte toda pessoa em capital humano – de si mesma, das empresas e de uma constelação econômica nacional ou pós-nacional, como a União Europeia. Consumo, educação, capacitação e escolha de parceiros são configurados como práticas de investimento em si mesmo, sendo o "si mesmo" uma empresa individual; e tanto o trabalho quanto a cidadania aparecem como modos de pertencimento à (equipe da) empresa na qual se trabalha ou à nação da qual se é membro. Empresas modernas buscam seus próprios interesses, é claro, mas de uma maneira específica. Longe de serem deliberadamente vorazes ou indulgentes, para conseguir sobreviver e prosperar precisam buscar estratégias cuidadosas de investimento, aprimoramento de capital, obtenção de vantagens, redução de custos, adaptação a ambientes em transformação, a novos desafios e às prolongadas altas nas taxas de crédito. Em outras palavras, elas não são entidades smithianas, meramente engajadas em "intercambiar e permutar",tampouco criaturas *benthamianas*, que simplesmente buscam o prazer e fogem da dor. Ao contrário, à medida que a racionalidade neoliberal refaz o sujeito humano como partícula do capital, há uma passagem da crua abordagem anterior do ser humano como maximizador de interesses, **para a formulação do sujeito ao mesmo tempo como membro de uma empresa e sendo ele mesmo uma empresa – apropriadamente conduzido, em ambos os**

> **casos, por estratégias de "governança" aplicáveis a empresas**. (BROWN, 2018, p. 5. Grifo nosso.)

A autora discute a maneira pela qual o conceito de *governança*, que adquire centralidade em nossa próxima seção, tornou-se onipresente e ambíguo, usado em contextos políticos, empresariais e institucionais para designar formas de organização que substituem leis e coerção por diretrizes, padrões e códigos de conduta. Trata-se de uma gramática que simula a descentralização do Estado, obscurecendo o exercício do poder na forma de uma terminologia técnica de gestão e boas práticas, em arranjos que combinam cooperação e isolamento. Brown recorda Foucault, nesse sentido, ao identificar uma lógica *omnes et singulatim* - que reúne e separa ao mesmo tempo - reforçando a autogestão e diluindo solidariedades coletivas.

Nesse registro, a noção de governança se apresenta como pós-política, deslocando debates sobre justiça, equidade ou legalidade para métricas de eficácia e eficiência, importando para o campo público a racionalidade empresarial de integração funcional e fungibilidade dos sujeitos (Brown, 2018). Assim, converte-se em prática despolitizadora que, ao mesmo tempo em que proclama neutralidade, naturaliza exclusões e assimetrias, alinhando indivíduos a projetos de nações, empresas ou universidades. No neoliberalismo, esse arranjo se articula à fusão entre Estado e capital na forma de parcerias público-privadas e intervenções financeiras que concentram e capilarizam o poder, socializando riscos e privatizando ganhos. Em suma, o que se observa é a intensificação de formas de dominação que, embora apresentadas em termos da cooperação e da técnica, reforçam o predomínio do capital financeiro e a erosão de referências externas – seja na forma da justiça democrática ou do bem comum – supostamente capazes de limitá-lo. A autora resume:

> Nas duas últimas décadas, a ideia e a linguagem da "governança" ascenderam aos circuitos acadêmicos, assim como a meios políticos, empresariais, agências públicas e organizações não governamentais. Governança não é o mesmo que neoliberalismo, não era parte do imaginário neoliberal estabelecido por Milton Friedman ou F. A. Hayek, e teve pouca participação nas transformações neoliberais da América de 1980. Porém, à medida que amadurecia e convergia com o neoliberalismo, a governança tornou-se sua principal forma administrativa, sem a qual o neoliberalismo contemporâneo é impensável. A tarefa, então, é apreender essa convergência de discursos e objetivos como sinergética e potente, ainda que não seja inevitável. Como conceito, a governança é frequentemente usada de forma intercambiável tanto com governar como com administrar. É também

> usado transversalmente na política, no mundo dos negócios e em instituições sem fins lucrativos, como universidades e complexos hospitalares. Essa promiscuidade é em si mesma um fenômeno léxico revelador: "governança", na verdade, indexa uma fusão específica de práticas políticas e empresariais. **Como ferramenta analítica, a governança descentraliza o Estado e monitora a dispersão de poderes organizados em todo o ordenamento social, poderes que conduzem e não apenas restringem o sujeito.** Referindo-se a políticas públicas, porém, a governança não hesita em substituir a formação e a implementação debatidas de políticas públicas pelo exercício aberto de autoridade e poder vernança, **"diretrizes" substituem leis, "facilitação" substitui regulamentação, "padrões" e "códigos de conduta" (disseminados por uma série de agências e instituições) substituem policiamento e outras formas de coerção estatal**. Juntas, essas substituições derrotam o vocabulário do poder, e consequentemente sua visibilidade para as vidas e os espaços que a governança ordena e organiza. (BROWN, 2018, p. 17. Grifos nossos.)

Nesse contexto, difunde-se um vocabulário técnico que traduz conflitos em metas, indicadores e "modos corretos de proceder", rebaixando leis a manuais e códigos, e a coerção explícita cede espaço a protocolos que parecem neutros. Mesmo agendas com forte teor igualitário — saúde, tributação, salário-mínimo, ciência, energia limpa — são justificadas preferencialmente por sua contribuição ao crescimento e à competitividade, reescrevendo a participação política como adesão a curvas de PIB. É pela retórica da renúncia "de todos", de uma cidadania sacrificial (Brown, 2018), convocando trabalhadores e usuários de serviços públicos a aceitarem cortes, congelamentos e perdas materiais como preço da estabilidade macroeconômica que o circuito decisório desloca encargos para instâncias cada vez menores — departamentos, escolas, municípios — a quem falta fôlego técnico e orçamentário, enquanto a imputação moral do fracasso passa a se concentrar nesses elos mais frágeis, operando portanto no isolamento de indivíduos entendidos como responsáveis em sua conversão na figura do empreendedor. Revela-se assim uma possível inversão do pacto protetivo que historicamente legitimou o Estado: já não se trata de blindar indivíduos contra riscos sistêmicos, *e sim de tornar indivíduos suportes de ajustes sistêmicos*. O cidadão é chamado a consumir, endividar-se, poupar ou aceitar rebaixamentos conforme a conveniência do ciclo econômico, internalizando a mensagem de que "fazer a sua parte" significa ajustar a própria vida à metas externas. Por trás dessa pedagogia pública, está em jogo uma tonalidade quase litúrgica: a oferta de si a um fim superior — o avanço dos indicadores — como prova de virtude cívica. Em síntese, uma linguagem que aparenta pragmatismo técnico desativa

disputas substantivas, naturaliza assimetrias e amplia a capacidade de exigir renúncias, ao mesmo tempo em que promete apenas eficiência (Brown, 2018).

Ao compreender, na mesma direção, o neoliberalismo como uma racionalidade de governo que reorganiza a economia política da vida, Chamayou (2020) acrescenta uma dimensão genealógica decisiva: a crise moral do liberalismo e a subsequente fundação de uma ética gerencial que passou a legitimar o poder econômico e político. Essa "crise teológica" decorrente da dissociação entre propriedade e controle, para o autor, abrirá espaço para a emergência de uma nova teodiceia secular: a crença na administração racional como princípio de governo. O gestor, desprovido da legitimidade do proprietário clássico, passa a ser investido de uma autoridade moral derivada da competência técnica. Essa transformação constitui a matriz ética das instituições multilaterais que, no pós-guerra, passaram a mediar a economia global — ONU, OCDE, FMI e Banco Mundial —, cuja autoridade se apoia na neutralidade técnica e na moralização da gestão. O deslocamento descrito por Chamayou — do proprietário ao gestor — reaparece na escala global como deslocamento do soberano ao especialista: organizações cuja força repousa sobre a credibilidade técnica e sobre dispositivos de *soft law*, isto é, normas que persuadem e coordenam condutas sem o recurso direto à coerção jurídica, cujos princípios de origem passam por transformações substantivas ao se adequar ao paradigma do livre mercado:

> A soft law teve origem numa batalha perdida, ao fim da qual seu significado e sua função política foram invertidos: de arma dos países do Sul, ela se transformou em escudo para as multinacionais do Norte. Para os antípodas da visão otimista do Dupuy, a soft law se tornou o principal instrumento de uma estratégia para evitar a regulamentação, visando à manutenção eterna de uma norma natimorta nos limbos do direito. Os mesmos que previram com preocupação essa nova arma potencial fizeram dela sua ponta de lança, ao destacar a ideia que, em matéria econômica, só seria possível ter, em escala internacional, um regime de direito especial, um "ramo autônomo menos conceitualizado e menos constrangedor, deslegalizado e desjurisdicionalizado", em que as "normas rígidas e precisas do direito internacional clássico parecem dar lugar […] às regras menos coatoras, e em que as regras "tendem a ceder o passo a programas, a normatividade à previsão, o direito puro e duro à soft law (...) só restaria a opção, leve e elegante, do código de conduta. (CHAMAYOU, 2020, p. 244)

A *soft law* internacional, nesse sentido, aparece como atualização contemporânea da *teodiceia* gerencial que Chamayou identifica nos anos 1930, ou seja, um poder que se afirma como racional e ético, mas que, de fato, opera pela administração de condutas e pela

imposição de padrões de comportamento em nome da eficiência e da segurança. Ao assumir a função de "árbitros morais" das práticas estatais e empresariais, instituições como a OCDE e a ONU se afirmam, também, como gestoras da moralidade neoliberal, regulando o campo global por meio de métricas, índices, códigos e recomendações, a partir dessa perspectiva. Essa forma de regulação moralizada — não coercitiva, mas performativa — reforça a tendência da governamentalidade neoliberal de substituir a soberania por mecanismos de autogoverno supervisionado. A genealogia proposta por Chamayou permite, portanto, situar a governança global da vigilância dentro de um mesmo processo histórico: o da transformação da moral liberal em ética gerencial, e da política em administração técnica. Nesse movimento, a vigilância e a coleta de dados aparecem como os instrumentos por excelência dessa nova economia moral: o gestor global precisa conhecer, prever e modelar os comportamentos — de empresas, de Estados, de populações — para assegurar a governabilidade da incerteza.

Essa lógica despolitizadora da governança encontra paralelo no campo da governança da internet, como veremos, onde instâncias como a ICANN, o Fórum de Governança da Internet (IGF) adotarão precisamente o mesmo vocabulário de "boas práticas", "cooperação multissetorial" e "facilitação". Como observa Laura DeNardis (2014), a governança da rede é estruturada em torno de arranjos técnicos e contratuais que mascaram disputas políticas, apresentando como "infraestrutura" escolhas que envolvem soberania, economia e desproporcionalidade. Nesse sentido, o diagnóstico de Brown ecoa na maneira como protocolos técnicos ou padrões de governança digital são tratados como neutros, ainda que organizem hierarquias geopolíticas e comerciais, como veremos na seção seguinte. (MUSIANI et al., 2016).

Trata-se também da mesma retórica de abertura e participação combinada à consolidação de poder em torno de grandes plataformas e consórcios técnicos, que concentram capacidade de definir padrões globais de interoperabilidade. Autores como Sérgio Amadeu da Silveira (2020) e Fernanda Bruno (2013) enfatizam que essa forma de regulação algorítmica opera justamente pela fusão entre Estado e mercado, transformando a internet em um laboratório do neoliberalismo por excelência, no qual direitos são traduzidos sobretudo em termos de condições de acesso. Nesse cenário, o consentimento emerge como tecnologia de subjetivação central, manifesta na obrigação de gerir termos de uso e políticas de privacidade, por meio de contratos, certificações e regimes de accountability que reforçam a referida dinâmica, transferindo ao indivíduo a suposta escolha por seu próprio

monitoramento, naturalizando assimetrias estruturais entre corporações e cidadãos. Em síntese, o paradigma neoliberal das sociedades da vigilância contemporâneas corresponde à sua reconfiguração em arranjos híbridos: corporações transnacionais assumem funções tipicamente soberanas de classificação e monitoramento; indivíduos são interpelados como sujeitos responsáveis por sua própria exposição; e o Estado aparece como mediador da concorrência global, o que parece conformar um terreno em que proteção, regulação e acumulação se confundem.

Essa racionalidade neoliberal, portanto, prepara o terreno para o debate sobre a governança global da internet e a proteção de dados. É nesse ponto de encontro entre neoliberalismo, vigilância e colonialismo de dados que se inscrevem as disputas exploradas no capítulo seguinte. Será justamente nesse duplo movimento - o de uma economia política da circulação de fluxos e uma matriz produtiva de modulação de possibilidades, que os sujeitos são progressivamente interpelados como gestores de si, agentes responsáveis pela administração estratégica de sua exposição a incerteza, enquanto a infraestrutura técnico-cibernética da segunda metade do século XX inaugura novas formas de ver, conhecer e governar a vida. É, portanto, da leitura combinada da governamentalidade neoliberal e virada tecnopolítica que procuramos interpretar transformação profunda nos regimes de visibilidade, tornando a privacidade não simplesmente uma categoria sob ameaça mas um dispositivo de governo, como veremos na seção 3.3.

Autores como Couldry e Mejias (2019) sugerem que essa configuração pode ser compreendida como uma forma de colonialismo de dados, na medida em que reitera a lógica de apropriação assimétrica de recursos – neste caso, informações – por parte de atores centrais em detrimento das periferias digitais. Na seção seguinte procuraremos situar o debate da governança como dimensão constitutiva desse mesmo processo, considerando a noção de colonialismo de dados como atualização de determinados modelos de governança e governabilidade em escala global, ancorados na capacidade de transformar fluxos informacionais em instrumentos de regulação e exploração. É nesse ponto de encontro entre o paradigma neoliberal, a governança digital e o colonialismo de dados que se inscreve o debate a ser explorado a seguir.

2.3 Governança, vigilância e algumas anotações sobre o colonialismo de dados

A noção de governança da internet constitui um dos eixos centrais para compreender tanto a dinâmica interna da rede em sua forma contemporânea quanto sua projeção na política internacional. Mais do que um arranjo de gestão técnica, trata-se de um campo que agrega múltiplos atores, arenas institucionais e instrumentos normativos que produzem efeitos concretos sobre dimensões tensionadas como soberania e privacidade. Conforme Walters (2004),

> Durante muito tempo utilizada como sinônimo de "governo", a palavra "governança" adquiriu, nos últimos dez anos aproximadamente, um novo status teórico e uma centralidade dentro dos estudos políticos. Um corpo crescente de trabalhos, cujo objetivo é mapear a transformação da ordem política, vem se consolidando sob o rótulo de governança. Em seu núcleo, essa literatura sobre governança — ou "nova governança" — sugere que a natureza do poder político mudou de forma bastante profunda. Ao contrário daqueles que, em certo momento, pediram que os estudos políticos "trouxessem de volta o Estado", a pesquisa sobre governança mostra-se cética quanto à centralidade conceitual e à validade do Estado. Os teóricos da governança argumentam que a era em que o Estado monopolizava e era sinônimo de governar está chegando ao fim, e que a imagem da autoridade emanando de um centro institucional fixo tornou-se ultrapassada. Em vez disso, sustentam que habitamos um mundo caracterizado pela governança. À medida que as sociedades se tornaram mais complexas e as demandas sociais se multiplicaram, a autoridade política tornou-se policêntrica e multinível. O governo não mais se exerce "sobre", mas sim em relação complexa com um campo denso de atores públicos e privados. (WALTERS, 2004, p. 27)

Como observa William Walters (2004), o vocabulário da "governança" que se consolida nos anos 1990 constituiria, à luz da racionalidade neoliberal, uma reconfiguração das técnicas de governo, que passam a operar sob a forma de coordenação e administração. Termos como *accountability*, *transparency* e *good governance* tornam-se categorias morais e performativas que legitimam a atuação de organismos internacionais como gestores, promotores de políticas de ajuste e disseminadores de métricas de eficiência e confiança institucional. Longe de significar a dissolução do poder estatal, essa governança global traduziria, em certo sentido, a extensão do ethos empresarial à esfera pública, deslocando a legitimidade da autoridade política para a competência técnica e o gerenciamento de riscos. Em sintonia com o "gerencialismo ético" de Chamayou (2020) a análise de Walters permite

situar as organizações internacionais como instrumentos centrais da moralização neoliberal do governo, através das quais a linguagem da boa governança passa a operar efetivamente como uma teologia secular da eficiência: converte o campo do político, objetivamente, em problemas de gestão.

No campo da Internet, foi estabelecido o lugar comum segundo o qual a governança tem como função central tanto a criação e manutenção das infraestruturas que permitem seu funcionamento contínuo quanto a formulação de políticas substantivas relacionadas a essas tecnologias (DeNardis, 2014). Esse arcabouço envolve múltiplas camadas técnicas que vão desde padrões de interoperabilidade e recursos críticos — como endereços de IP e o sistema de nomes de domínio (DNS)[13] —, entre outros. Tomando esse panorama como referência, pode-se delinear, para Laura DeNardis (2014) cinco dimensões que estruturam a análise da governança global da Internet: (1) o modo como a configuração técnica funciona como configuração de poder; (2) a utilização desses mecanismos como substitutos para controle de conteúdos; (3) o avanço da privatização da governança digital; (4) a disputa em torno de pontos estratégicos da rede como arenas de conflito global e de valores concorrentes; e (5) as tensões permanentes entre dinâmicas locais de poder e a natureza transnacional da rede. De início, partimos aqui do pressuposto de que estamos falando da própria base sobre a qual se organiza o capitalismo de vigilância, a partir de camadas técnicas que permitem a circulação e centralização de dados, progressivamente colonizadas por corporações que as utilizam para extrair excedente comportamental.

DeNardis, ainda, ressalta que longe de se restringir a um campo de intervenção direta do Estado, desenvolve-se em um conjunto articulado de arranjos privados, soluções técnico-institucionais e práticas transnacionais que assumem protagonismo. Embora governos continuem a estabelecer marcos regulatórios – seja na proteção de dados, na regulação concorrencial ou no enfrentamento a ilícitos digitais –, grande parte das funções de normatização e controle é exercida por corporações privadas e entidades técnicas. A própria arquitetura da rede, composta por padrões de interoperabilidade, endereçamento e mecanismos de intermediação informacional, configura relações de poder que transcendem

[13] se refere a infraestrutura que traduz nomes legíveis para endereços IP, representados originalmente em números binários (sequências de 0 e 1) que identificam de forma única cada dispositivo conectado à Internet. Esses endereços permitem que pacotes de dados cheguem ao destino correto.. Ou seja, o DNS funciona como uma "lista telefônica da Internet" em vez de digitarmos o número binário do servidor, usamos um nome fácil de memorizar, e o DNS faz a correspondência para o endereço técnico real.

fronteiras territoriais, evidenciando que a regulação se dá tanto por dispositivos jurídicos quanto por protocolos técnicos que estruturam fluxos e condicionam práticas. A autora resume,

> Grande parte da governança da Internet é exercida por corporações privadas e entidades não governamentais. Por exemplo, as especificidades da privacidade individual online são definidas pelos termos de uso de plataformas de mídia social e pelas práticas de coleta e retenção de dados da indústria de publicidade digital, dos mecanismos de busca e de outros intermediários da informação. Como se observou no exemplo de protestos na Internet apresentado anteriormente, a ação coletiva de cidadãos privados, bem como boicotes de alto perfil promovidos por empresas, também pode influenciar as decisões de governança da Internet. Nesse sentido, o setor privado exerce influência não apenas por meio das políticas que estabelece para o uso de seus produtos e serviços, mas também sobre ações governamentais tradicionais.Empresas privadas como a VeriSign atuam como registradoras de nomes de domínio, operando componentes vitais das infraestruturas da governança da Internet. As companhias de telecomunicações privadas constituem a maior parte da espinha dorsal da rede e se conectam entre si por meio de acordos contratuais privados firmados em pontos de troca de tráfego. Assim, as corporações privadas não apenas executam políticas ao desempenhar suas funções centrais, mas também agem como atores políticos, respondendo a eventos e disputas que ocorrem em um palco político mais amplo. (DeNARDIS, 2014, p. 12. Tradução nossa.)

Nesse contexto, observa-se uma tendência de delegação de funções tradicionalmente estatais a atores privados, que passam a exercer papéis centrais na moderação de conteúdos, na entrega de dados para autoridades públicas ou na manutenção de infraestruturas críticas. Casos como a suspensão dos serviços do WikiLeaks[14] por provedores de hospedagem, empresas de DNS e intermediários financeiros ilustram o exercício de poder político por corporações sem a mediação de limites constitucionais. Essa dinâmica insere-se em processos mais amplos de privatização e desestatização, em que empresas transnacionais adquirem capacidade de definir políticas públicas de facto, influenciando regulações em setores estratégicos e moldando direitos fundamentais como a liberdade de expressão e a privacidade. Iniciativas de autorregulação – como a Global Network Initiative[15] – buscam conferir

[14] Em 2010, após a publicação de telegramas diplomáticos norte-americanos pela plataforma, diversas empresas privadas — como Amazon, PayPal, Visa e MasterCard, além de provedores de DNS — decidiram interromper unilateralmente os serviços oferecidos ao WikiLeaks. Esse episódio demonstrou de forma clara que atores privados, mesmo sem um mandato governamental formal, exercem poder político significativo ao condicionar o acesso a infraestruturas essenciais da rede. Em outras palavras, evidenciou que a governança da Internet não se limita a normas estatais ou tratados internacionais, mas é marcada por formas de governo delegado ou governo privatizado, em que corporações controlam pontos estratégicos da rede e tomam decisões com impactos diretos sobre liberdade de expressão, fluxo de informações e direitos fundamentais.

[15] Trata-se de uma coalizão multissetorial criada em 2008 que reúne grandes empresas de tecnologia (como Google, Microsoft, Yahoo!), organizações da sociedade civil, investidores e acadêmicos. Seu objetivo central é estabelecer princípios e diretrizes para a proteção dos direitos humanos na Internet, sobretudo a liberdade de

legitimidade a essas práticas, mas não eliminam a opacidade e as assimetrias inerentes a um regime no qual a governança digital é exercida por meio da coprodução de normas entre Estados e corporações, sob condições de poder difusas e frequentemente despolitizadas.

Uma concepção simplista da governança da Internet tende a imaginar que autoridades públicas definem metas e que engenheiros se limitam a executá-las de forma neutra. Essa formulação, contudo, negligencia a força de interesses políticos e econômicos, a participação ativa de mercados e comunidades de usuários e os efeitos inesperados que atravessam qualquer projeto técnico que, de fato, co-produzem normas, identidades e regimes de verdade (Jasanoff, 2004; Denardis, 2014). A reflexão clássica de Langdon Winner (1980), em *Do Artifacts Have Politics?*, converge nesse sentido, ao sustentar que artefatos carregam implicações políticas próprias, capazes de reorganizar práticas coletivas e delimitar relações de poder.

No terreno da Internet, a exigência de unicidade global para endereços e nomes de domínio não representou apenas uma escolha técnica; instituiu, ao mesmo tempo, arenas de disputa sobre quem detém legitimidade para coordenar recursos críticos, tensões que marcam os embates em torno da governança desde os anos 1990. Esse entrelaçamento entre arquitetura técnica e política se revela também na análise de protocolos. Dispositivos concebidos para viabilizar o compartilhamento distribuído de arquivos, tornaram-se indissociáveis de embates sobre propriedade intelectual e pirataria digital e mesmo técnicas de gestão de tráfego, quando baseadas em inspeção profunda de pacotes, evidenciam a presença de valores e escolhas normativas. O debate em torno de legislações como SOPA/PIPA[16] ilustra essa dinâmica, sugerindo que ao se alterar a configuração material da

expressão e a privacidade, em um cenário de pressões crescentes de governos que solicitam a remoção de conteúdos, o bloqueio de serviços ou a entrega de dados de usuários. A GNI surgiu como resposta a episódios em que empresas de tecnologia foram criticadas por colaborar com censura ou vigilância estatal — por exemplo, quando mecanismos de busca ou provedores de e-mail ajustaram seus serviços para se adequar às exigências de regimes autoritários. A iniciativa elaborou um conjunto de princípios baseados em normas internacionais de direitos humanos (como a Declaração Universal dos Direitos Humanos e o Pacto Internacional sobre Direitos Civis e Políticos), oferecendo procedimentos de due diligence, relatórios de transparência e auditorias independentes para que as empresas participantes demonstrem como equilibram demandas governamentais com a proteção de direitos. Na prática, a GNI representa uma forma de auto regulação transnacional no campo da governança da Internet, produzindo padrões voluntários de conduta, que ao mesmo tempo reforçam a legitimidade corporativa diante de críticas e servem como espaço de negociação entre empresas, sociedade civil e governos. Para alguns críticos (DeNARDIS, 2014), trata-se de um exemplo da privatização da regulação global, em que atores privados assumem papéis tradicionalmente estatais na definição e aplicação de normas, refletindo a ambivalência entre proteção e captura que caracteriza a governança neoliberal da rede.

[16] O debate em torno das legislações SOPA (*Stop Online Piracy Act*) e PIPA (*Protect IP Act*), apresentadas no Congresso dos Estados Unidos em 2011–2012, diz respeito às tentativas de combater a pirataria digital e

Internet — seus protocolos, padrões e camadas de infraestrutura —, transformam-se também as formas de governança possíveis, os modos de visibilidade e as condições de ação coletiva em escala global.

Como observa Pigatto (2024), o caráter multissetorial da Internet, desde sua constituição, ao mesmo tempo implica numa lógica profundamente assimétrica de compartilhamento de responsabilidades entre governos, empresas, sociedade civil e comunidade técnica. Não há, entretanto, consenso definitivo sobre como delimitar esse regime, enquanto parte da literatura tende a descrevê-lo como marcado por interdependências e tensões entre diferentes camadas — da infraestrutura física ao conteúdo que circula nas plataformas, outras abordagens enfatizam a noção de um "complexo de regimes", proposta por Nye (2014), no qual múltiplos espaços institucionais, formais e informais, interagem sem convergir para uma autoridade centralizada. O autor exemplifica:

> É improvável que venha a existir, em um futuro próximo, um regime único e abrangente para o ciberespaço. Atualmente há um alto grau de fragmentação, e é provável que essa condição persista. O cenário mais plausível é a evolução de um complexo de regimes — uma configuração intermediária entre uma estrutura jurídica unificada e uma fragmentação completa das normas.Questões distintas tendem a se desenvolver em ritmos diferentes, com alguns temas avançando e outros retrocedendo nas dimensões de profundidade, abrangência e conformidade. Algumas áreas, como a do crime cibernético, nas quais os Estados possuem interesses comuns contra terceiros que se beneficiam de forma oportunista (*free riders*), parecem propícias a acordos interestatais — ainda que apenas para cooperação em esforços legais e forenses. Outras questões, como a privacidade, podem dar lugar a compromissos no contexto de negociações comerciais, que formalmente não têm conexão direta com o domínio cibernético. E algumas áreas, como a guerra cibernética, talvez não sejam suscetíveis a acordos formais de controle de armamentos, mas podem ver surgir políticas declaratórias, medidas de fortalecimento de confiança e regras gerais de conduta.

proteger direitos autorais por meio de mecanismos de bloqueio de conteúdos na Internet. Esses projetos previam que autoridades poderiam obrigar provedores de acesso, motores de busca e intermediários financeiros a cortar conexões com sites acusados de violar propriedade intelectual, mesmo que localizados fora dos EUA. Em termos práticos, isso significaria usar a arquitetura técnica da Internet como instrumentos de censura e controle. Grandes conglomerados de mídia e entretenimento defenderam os projetos, alegando perdas bilionárias decorrentes da pirataria, enquanto empresas de tecnologia, ativistas digitais e acadêmicos denunciaram riscos à liberdade de expressão, à inovação e à própria integridade técnica da rede, já que o bloqueio de domínios poderia fragmentar o sistema global da rede. As críticas culminaram em protestos online de grande escala em janeiro de 2012, incluindo o "apagão" de sites como a Wikipédia e o Google, que mobilizaram milhões de usuários contra as propostas. Como resultado, SOPA e PIPA foram arquivadas, tornando-se marcos de um embate maior sobre até que ponto governos e corporações podem intervir na infraestrutura da Internet para regular conteúdos — embate que permanece no centro da discussão sobre governança digital.

> Em vez de acordos globais, Estados com visões convergentes podem agir conjuntamente para evitar comportamentos desestabilizadores e, posteriormente, tentar generalizar essas práticas a um grupo mais amplo de atores, por meio de diferentes meios — desde negociações formais até cooperação e assistência para o desenvolvimento. (NYE, 2014, p. 15. Tradução nossa.)

Ambas as formulações, ainda que divergentes, trazem luz a uma importante especificidade desse debate ao sugerir que a Internet não se enquadra facilmente nos modelos tradicionais de governança global, sendo simultaneamente mais fragmentada e, ao mesmo tempo, mais interconectada que outras áreas da cooperação internacional, revelando disputas constantes entre lógicas de universalidade e estratégias de fragmentação (Rocillo et al., 2021; Santaniello, 2021; Van Eeten et al., 2013). É nessa chave que fóruns como o Fórum de Governança da Internet (IGF) e a União Internacional de Telecomunicações (UIT) devem ser lidos não como instâncias isoladas, mas como arenas que materializam dilemas estruturais. O IGF, criado em 2005 na Cúpula Mundial da Sociedade da Informação, foi concebido como inovação institucional multissetorial, buscando superar a percepção de que a internet era governada apenas por atores técnicos e estatais.

Em contraste, a UIT ilustra a continuidade de mecanismos intergovernamentais clássicos. Sua longa trajetória como agência das Nações Unidas e sua capacidade de produzir normas técnicas com peso jurídico a colocam em um espaço privilegiado do debate da governança da internet, considerando que opera a partir de instrumentos formais de deliberação que produzem eficácia normativa em torno da centralidade do Estado na definição da agenda. Essa característica, que lhe confere força regulatória, aparece na literatura também como seu maior ponto fraco, uma vez que marginaliza a participação de atores não estatais, tendendo a privilegiar interesses soberanos e securitários (DeNardis, 2014), deixando em segundo plano a pluralidade de demandas que marcam o hibridismo característico da rede. Entre os dois casos paradigmáticos, a trajetória do Internet Corporation for Assigned Names and Numbers (ICANN), marcado por sua natureza híbrida, é alvo de críticas recorrentes. Pigatto (2024, p. 201), nessa direção, destaca que *"a ICANN foi por muito tempo acusada de representar a hegemonia estadunidense sobre funções críticas da rede, dada sua vinculação inicial ao Departamento de Comércio dos EUA*", mas lembra que a transição concluída em 2016 buscou mitigar essa percepção. Ainda assim, segundo Nye (2014 apud Pigatto, 2024), persistem assimetrias, já que a governança técnica continua dependente de recursos e expertise concentrados em poucos centros. A ICANN exemplifica,

assim, as ambiguidades de um modelo privado sem fins lucrativos que exerce funções com impactos diretos sobre soberania e economia global.

A leitura integrada desses quatro arranjos nos permite inferir que não há um modelo único de governança, havendo de fato uma constelação de instituições que materializam dilemas constitutivos. O IGF enfatiza a legitimidade inclusiva, mas carece de eficácia normativa; A UIT dispõe de autoridade formal, mas mantém déficit de abertura a atores não estatais; A ICANN demonstra eficiência técnica, embora carregue assimetrias históricas vinculadas a hegemonia estadunidense, enfim: um conjunto de tensões entendidas como permanentemente estruturante do campo (Pigatto, 2024).

Nota-se, ainda, que embora a lógica da soberania nacional permaneça preponderante, empresas transnacionais e arranjos normativos extraterritoriais produzem constrangimentos que ultrapassam fronteiras. A GDPR europeia, como trataremos no Capítulo 3, ao projetar seus princípios de proteção de dados sobre o resto do mundo, exemplifica esse processo de exportação regulatória. Ao mesmo tempo, iniciativas chinesas de localização de dados e censura digital expressam uma concepção distinta, ancorada em segurança nacional e soberania informacional. Essas estratégias contrastantes revelam que a governança contemporânea da internet corresponde sobretudo a uma expressão de disputas geopolíticas e de modelos de ordem internacional concorrentes.

A literatura também evidencia divergências conceituais quanto ao papel das plataformas digitais. Para alguns autores, elas constituem simples intermediárias de conteúdo; para outros, aproximam-se de instituições com poder normativo equiparável ao de Estados ou organismos internacionais, representando espaços de socialização política e econômica de produção de regimes próprios de regras e sanções. A moderação de conteúdo, nesse contexto, ilustra a dificuldade de definir fronteiras claras entre regulação estatal e autorregulação privada. Não é irrelevante que as práticas de governança da internet estejam cada vez mais permeadas por crises de confiança, principalmente à luz dos episódios que revelam práticas de vigilância em massa, conforme tratamos no item 1.3. O quadro que identificamos, portanto, é o de uma governança em tensão, ao mesmo tempo marcada por discursos em defesa do multissetorialismo e da universalidade, princípios orientadores dos principais fóruns que permanecem servindo de horizonte normativo e, por outro lado, por um conjunto

de tendências à fragmentação e à securitização que persistem em tensionar esse mesmo horizonte.

A virada provocada pelos vazamentos de Edward Snowden, em 2013, é difícil de ser superestimada nesse enquadramento, em termos de uma "nova era" na governança da internet, elevando a governança de dados pessoais e da privacidade a uma das principais agendas dos fóruns de governança da Internet, pautando com força temas em torno da proteção de dados pessoais, as leis de acesso à informação, o uso de inteligência artificial, o gerenciamento e tratamento de dados, seu uso legítimo e bases legais e a transferência de dados entre atores a nível global (United Nations, 2023; United Nations, 2019; Llanos, 2022,).

No plano normativo, a inflexão é visível já em dezembro de 2013, quando a Assembleia Geral aprova a Resolução 68/167 e, de forma inédita, faz um chamamento aos Estados a reverem leis, práticas e procedimentos de vigilância — inclusive em larga escala — à luz do direito internacional dos direitos humanos, com ênfase em transparência, supervisão independente e responsabilização. O documento também solicitou ao Alto Comissariado um relatório específico sobre "o direito à privacidade na era digital", abrindo um ciclo de acompanhamento que perdura até hoje, tendo ao longo do tempo diagnosticado lacunas legislativas, salvaguardas fracas e fiscalização insuficiente em diversos países, cenário que tornaria difícil avaliar a legalidade e a proporcionalidade de políticas de interceptação e coleta de dados (UN, 2013; OHCHR, 2014). A partir desse momento, os debates não se restringiram à interceptação de comunicações, tendo se voltado na década seguinte também a práticas de *hacking* estatal e comercial, criptografia e monitoramento de espaços públicos. O relatório do ACNUDH ao HRC em 2022 (A/HRC/51/17) explicita esse tripé — chamando atenção para o abuso de ferramentas intrusivas, o papel protetivo da criptografia e a vigilância pervasiva de espaços físicos (OHCHR, 2022).

A leitura conjunta dos referidos diagnósticos gerou, em resposta, a consolidação de uma gramática de princípios e limites em torno de princípios de legalidade, finalidade legítima, necessidade, proporcionalidade, não discriminação e salvaguardas robustas. A eles somaram-se recomendações operacionais, como a restrição do reconhecimento biométrico em espaços públicos a crimes graves e sob estrito cumprimento de requisitos, além de considerar, dada a gravidade dos impactos de seu uso excessivo, moratória na venda e uso de ferramentas

de interceptação e *hacking* até que se verifique um regime de garantias baseado em direitos humanos. A Resolução 77/211 (2022) recupera e aprofunda esse arco, reafirmando que vigilância ilegal ou arbitrária — inclusive extraterritorial e/ou em massa — representa violação direta ao direito à privacidade e pedindo escrutínio renovado dos agentes públicos sobre sua adoção indiscriminada. Em paralelo, cresce o entendimento de que proteger a criptografia, a anonimização e o sigilo das comunicações não corresponderia a um luxo de especialistas técnicos, mas uma condição para o exercício de vários outros direitos (UNGA, 2022; Privacy International, 2024).

Esse movimento, por óbvio, não eliminou contradições. Segurança nacional, inovação tecnológica e direitos fundamentais representam eixos de um equilíbrio artificial, instável e desarmônico, e as trajetórias nacionais divergem — a ponto de a literatura falar em "modelos" concorrentes (sobretudo em torno dos casos estadunidense, europeu, chinês) irradiadores de preferências regulatórias e técnicas para foros como IGF, UIT e iniciativas ligadas ao sistema ONU (UNITED NATIONS, 2023; UNITED NATIONS, 2019). É plausível sustentar que a pressão pós-Snowden abriu espaço para contrapesos institucionais e para regulações extraterritoriais (como as europeias), sem, porém, suprimir o apetite de Estados e mercados por soluções intrusivas, tendo sido acompanhada por chamadas para regular a venda, a transferência e a exportação de tecnologias de vigilância e para instituir uma nova agenda regulatória da vigilância e da privacidade. Convém ressaltar que esse deslocamento é com frequência interpretado como, também, um contexto de inflexão quanto aos papéis de atores não estatais, tendo tensionado as grandes plataformas digitais para revisão de estratégias, implementação de políticas de transparência sobre pedidos de dados pelo setor público e demandado protocolos robustecidos de criptografia ponta-a-ponta. Entretanto, como destacam relatórios da Privacy International (2024), trata-se de respostas ambíguas, na medida em que representam em certo sentido vitórias de grupos da sociedade civil organizada que advogam por maiores dispositivos normativos de proteção, podendo de igual maneira ser lidas como tentativas de blindar a legitimidade corporativa diante de consumidores globais. Nesse cenário, a distinção entre "vigilância estatal" e "vigilância privada" torna-se cada vez mais porosa, o que amplia a complexidade do debate sobre governança e exige novos mecanismos de *accountability* multissetorial (Privacy International, 2024).

Nesse cenário, as Nações Unidas enfatizam princípios normativos universais em suas resoluções sobre privacidade e vigilância digital, insistindo na necessidade de garantias ao mesmo tempo em que as práticas nacionais demonstram que a governança da Internet e da proteção de dados se organiza a partir de trajetórias distintas, refletindo projetos regulatórios em competição. Pelo Regulamento Geral de Proteção de Dados (GDPR), sobre o qual nos debruçarmos no próximo capítulo, a União Europeia se consolida como protagonista normativo no estabelecimento de regras para coleta, tratamento e transferência de informações pessoais, projetando rapidamente sua influência para além das fronteiras regionais por meio de mecanismos de adequação, pelos quais países terceiros devem alinhar suas legislações à norma europeia para manter fluxos comerciais e digitais.

A experiência norte-americana é distinta (DeNardis, 2014; Pigatto, 2024). Em vez de um marco regulatório abrangente, prevalece um sistema fragmentado, baseado em legislações setoriais (como a *Health Insurance Portability and Accountability Act* para saúde, ou a *Children's Online Privacy Protection Act* para proteção de dados infantis), complementado por regimes de auto regulação corporativa. Nesse contexto, segurança nacional e inovação tecnológica ocupam lugar prioritário, relegando as garantias de privacidade a mecanismos limitados e, por vezes, reativos, compatíveis com a caracterização do fenômeno do capitalismo da vigilância, na medida em que privilegiam o dinamismo da circulação de dados em função da plataformização da economia. Frequentemente apresentada em oposição ao modelo americano, a literatura tem trazido luz para o caso da China (Hurrell et al., 2021), mobilizado em torno de uma noção de soberania digital, onde o Estado desempenha papel central tanto no controle das infraestruturas críticas quanto na definição do que é considerado aceitável em termos de circulação de informações. A Lei de Cibersegurança de 2017, combinada a mecanismos de censura digital como o chamado "Grande Firewall", confere ao governo instrumentos extensivos de vigilância e monitoramento.

A coexistência desses três modelos — europeu, estadunidense e chinês — projeta-se de forma direta no campo da governança global. Não se trata de arranjos paralelos, mas de projetos que competem pela definição de padrões, princípios e legitimidade normativa. À luz do exposto, é possível um deslocamento da análise da governança da Internet em termos dos regimes de enunciação que a estruturam. Fóruns multissetoriais ou intergovernamentais, como o IGF e a UIT, dessa perspectiva, tenderiam a operar menos como espaços neutros de coordenação técnica e mais como instâncias produtoras de critérios de legitimidade, em que

se define o que conta como verdade e quais práticas podem ser validadas institucionalmente. Nesse sentido, se trata de compreender como a própria noção de autoridade é continuamente reelaborada em gramáticas técnicas que assumem aparência de neutralidade. Pigatto (2024), ao enfatizar a disputa em torno da legitimidade, sugere que essas arenas funcionam como materializações de dilemas estruturais sobre quem pode falar em nome da rede e sob quais condições. A fragmentação da governança, frequentemente interpretada pela literatura como evidência de déficit institucional ou incapacidade de coordenação global, pode ser descrita, a partir de uma chave genealógica, menos como falha do sistema e mais como arranjo estratégico de redistribuição do poder. Em lugar de se traduzir pura e simplesmente em ausência de autoridade central, essa multiplicação de fóruns e camadas normativas tende a funcionar como tecnologia política voltada à administração da pluralidade, produzindo mecanismos que dispersam, mas também estabilizam, práticas de vigilância e de regulação, recuperando de Foucault (1999) a hipótese de que proliferação de arenas não dissolve a circulação do poder, pelo contrário - reconfigura suas modalidades de atuação e seus efeitos de normalização.

No pós Snowden (DeNardis, 2014; Santaniello, 2021), o discurso da descentralização passa a evocar simultaneamente a retórica da autonomia e a contestação das assimetrias vinculadas ao modelo estadunidense, ao mesmo tempo em que opera como mecanismo de recomposição da legitimidade de práticas de vigilância em seus arranjos contemporâneos, rearticulando as condições de aceitabilidade de determinadas práticas e deslocando dispositivos já existentes para fóruns multilaterais, revestindo-os de uma linguagem de participação ampliada e de salvaguardas jurídicas. Nessa lógica, a fragmentação tende a configurar-se como a capilarização ampliada do exercício do poder, reinscrevendo desigualdades estruturais sob gramáticas que se apresentam em chave de inclusão e consenso (UNITED NATIONS, 2023; UNITED NATIONS, 2019).

As plataformas digitais constituem, nesse cenário, um objeto analítico particularmente fértil. Elas podem ser descritas (DeNardis, 2014) como infraestruturas normativas que estabelecem regimes próprios de regulação, organizando práticas de moderação e algoritmos de visibilidade que configuram experiências sociais e políticas, constituindo um terreno condições de possibilidade para a ação. Nesse sentido, a tensão entre regulação estatal e autorregulação corporativa pode ser interpretada menos como racionalidade de governo que opera justamente no entrelaçamento entre segurança e liberdade (Manokha, 2009). Sob essa

ótica, a governança da Internet pode ser descrita como tecnologia voltada à administração contínua de crises, em que episódios de vulnerabilidade - talvez expressos em sua forma mais evidente com os vazamentos de Edward Snowden - não configuram rupturas externas, mas funcionam como elementos constitutivos dessa própria racionalidade. A repetida alegação de uma crise da privacidade, nesse sentido, aparece como uma engrenagem que autoriza a expansão de dispositivos regulatórios e tecnopolíticos, conferindo legitimidade a mecanismos que intensificam a captura de dados, convertendo a promessa de proteção em vetor de novas práticas de monitoramento.

Desse modo, a governança da Internet pode ser interpretada como espaço de produção de subjetividades e de normalizações (Brown, 2018), em que crises não se encerram em soluções definitivas, mas são continuamente mobilizadas como motores de reconfiguração e de reforço das tecnologias de governo. O vocabulário dos direitos humanos (Manokha, 2009) contribui, aqui, como um paralelo interessante, na medida em que estabelece padrões de aceitabilidade, molda a linguagem das práticas estatais e corporativas e fornece gramáticas de legitimidade que os próprios violadores invocam para justificar suas condutas. Algo semelhante se observa no campo da Internet, no qual a retórica da governança multissetorial se apresenta como horizonte incontornável, ainda que as práticas concretas mantenham assimetrias profundas. O recurso a fóruns como o IGF e a constante reafirmação da transparência e da participação plural (United Nations, 2019) podem ser interpretados, nessa direção, como mecanismos de autojustificação que ocultam, sem eliminar, a persistência de relações hierárquicas. Essa simetria entre discursos sugere que a governança digital, à semelhança do campo dos direitos humanos, tende a produzir consensos retóricos. Contudo, esse consenso - como discutido em seções anteriores - convive com práticas de vigilância intensificadas, resultando em um campo no qual a denúncia e a legitimação se imbricam. Trata-se, em certo sentido, de um jogo de verdade que, mais do que resolver contradições, as mantém produtivas e operacionais.

Ao mesmo tempo, a universalidade proclamada por esses referidos consensos - sobretudo, para o que aqui nos concerne, sobre a privacidade e a proteção de dados convive com fluxos assimétricos de extração de dados, em que o Sul Global permanece como provedor de insumos e o Norte Global como produtor de normas e tecnologias. Remetendo a processos concretos de apropriação de recursos vitais — neste caso, informações pessoais e coletivas — que, historicamente, reproduzem padrões de dominação e exploração típicos do

colonialismo clássico, o colonialismo de dados (Couldry e Mejias, 2019) representa uma nova etapa da acumulação, em que a vida social em sua totalidade é convertida em insumo para a geração de valor econômico e político, por meio de processos organizados de forma desigual, beneficiando determinados atores e subordinando populações e Estados com menor capacidade de regulação e infraestrutura. Em vez de terra ou trabalho, são os rastros digitais de interações, preferências e afetos que passam a ser colonizados, armazenados e explorados.

No contexto latino-americano, Cassino et al. (2023) trabalham essa análise ao destacar que o colonialismo de dados reitera relações de dependência históricas. Assim como os ciclos de exploração de recursos naturais, a extração massiva de dados ocorre em fluxos assimétricos, nos quais o Sul Global fornece matéria-prima informacional sem controle efetivo sobre seu destino e, nesse sentido, é também uma forma de colonialidade epistêmica, na medida em que determina o que é conhecimento válido e quais dados são relevantes a partir de perspectivas hegemônicas. Para compreender a pertinência da noção de colonialismo de dados, é fundamental resgatar como práticas de classificação e quantificação foram, desde a experiência do empreendimento colonial moderno, instrumentos da intervenção europeia. O censo, por exemplo, estruturava modos de ver e governar populações, estabelecendo categorias raciais, étnicas e territoriais que reforçavam hierarquias coloniais, do mesmo modo em que mapas operavam como tecnologias de dominação que projetavam fronteiras, definindo quais territórios eram legíveis para a administração imperial e quais comunidades poderiam ser integradas ou marginalizadas. Nesse sentido,

> O colonialismo histórico e o colonialismo de dados compartilham algumas estruturas fundamentais que sustentam tanto as formas de apropriação de recursos quanto as relações sociais de cada um: o modo como o sujeito colonizado é conceitualizado e como o colonialismo molda a maneira pela qual os colonizados pensam a si mesmos; a naturalização de certos modos de governar os sujeitos; e a legitimação de determinados tipos de conhecimento com suas respectivas pretensões de poder — incluindo uma conceitualização específica de tempo e espaço que acaba por universalizar uma visão de mundo particular. Se o colonialismo histórico consistiu na apropriação da terra, dos corpos e dos recursos naturais, o colonialismo de dados pode ser entendido como uma apropriação dos recursos sociais, representando ao mesmo tempo um avanço do capitalismo e um retorno potencial a formas mais brutais de exploração. É justamente porque a despossessão dos recursos sociais, hoje, opera de maneiras que replicam a antiga despossessão dos recursos naturais que podemos afirmar que as relações de dados recriam uma forma colonizadora de poder. As relações de dados são novos tipos de relações humanas que oferecem às corporações uma visão abrangente de nossa sociabilidade, permitindo que a vida humana se torne um insumo

> ou recurso para o capitalismo. Nesse esquema neocolonial, a colônia não é mais um espaço geográfico, mas uma "realidade aumentada" na qual conduzimos nossas interações sociais sob condições de extração contínua de dados. Os recursos que estão sendo colonizados são as associações, normas, códigos, saberes e significados que nos permitem manter conexões sociais, os processos humanos e materiais que constituem a atividade econômica, e o espaço subjetivo a partir do qual nos relacionamos com o mundo social. (COULDRY e MEJIAS, 2019, p. 85. Tradução nossa.)

Couldry e Mejias (2019) sugerem que a lógica contemporânea da dataficação da vida social guarda paralelos diretos com esses dispositivos históricos. Se antes a preocupação era mapear terras e populações para extrair recursos materiais, hoje a coleta massiva de dados busca capturar dimensões imateriais da vida cotidiana. Trata-se de uma continuidade em que a apropriação de informações é condição para consolidar formas de controle político e acumulação econômica (SILVEIRA et al., 2021; COULDRY e MEJIAS, 2019; SCOTT, 1998). O que muda, entretanto, é a escala: o *big data* amplia a abrangência das práticas de classificação a níveis micro, incorporando padrões de consumo, circulação, afetos e redes de interação. Essa continuidade histórica, os autores ressaltam, não significa repetição linear, pelo contrário, haveriam deslocamentos fundamentais. Para o colonialismo moderno, o censo e a cartografia, por exemplo, serviam sobretudo para afirmar a soberania territorial e justificar políticas de exploração direta. No colonialismo de dados, por sua vez, as fronteiras territoriais tornam-se menos relevantes do que os fluxos informacionais. A extração ocorre de maneira difusa, atravessando dispositivos pessoais, plataformas digitais e sistemas de vigilância distribuídos (Couldry e Mejias, 2019; Ricaurte, 2019). Embora, nesse sentido, a lógica de captura se mantenha, as infraestruturas e as justificativas se transformam. Se antes o discurso legitimador era o da civilização e do progresso, hoje recorre-se à retórica da inovação, da eficiência e da segurança. O percurso recuperado pelos autores, entretanto, procura reforçar como as formas de classificar e ordenar populações produziram efeitos materiais duradouros que sustentaram políticas discriminatórias e, na forma dos algoritmos contemporâneos, reproduzem vieses que, embora naturalizados como resultados técnicos, operam gramáticas de exclusão que instituem realidades. Evidenciam, nesse sentido, que a neutralidade dos dados é, tanto no passado quanto no presente, não mais do que uma ficção política.

Os autores, ainda, descrevem o fenômeno como um processo de construção de um imaginário de habitabilidade (Couldry e Mejias, 2019b), isto é, um conjunto de narrativas, práticas e justificativas que normalizam a apropriação contínua de fluxos de dados como

condição para a vida contemporânea, enfatizando uma dimensão de legitimação cultural e política que permite as grandes plataformas a transformação da vigilância em rotina, convertendo a coleta pervasiva em elemento constitutivo da experiência social. A contribuição dos autores é particularmente relevante para problematizar a falsa oposição entre proteção e controle, ao evidenciar que ambos se inscrevem em um mesmo regime de governabilidade digital. O discurso da proteção da privacidade não elimina a expropriação, mas participa da construção de sua habitabilidade, posto que a promessa de segurança e transparência funcionam como sustentadores da aceitação social da captura contínua desses fluxos, em torno de um campo de produção de subjetividades dispostas a consentir com a sua permanência, não por acaso coerentes com a forma atual dos discursos correntes sobre a governança global da Internet.

Souza (2024), no interior deste debate, propõe que regular a economia de dados não seria traduzível exclusivamente em uma questão técnica, mas em um projeto político que exige a descolonização dos próprios fundamentos normativos de regulação do digital. Para o autor, as arquiteturas jurídicas globais reproduzem hierarquias coloniais sob o disfarce de universalismo, ao pressuporem um sujeito informacional abstrato, individualista e proprietário de seus dados. A alternativa de Souza é proposta em termos da construção de regimes de governança ancorados na pluralidade epistêmica e territorial dos povos e comunidades que produzem e são produzidos pelos dados, implicando no abandono do paradigma da proteção individual para adotar o da redistribuição do poder informacional (Souza, 2024). De modo complementar, Couldry e Mejías (2019), ao historicizar o vínculo entre capitalismo e colonialismo, eles demonstram que a promessa contemporânea de governança ética — centrada na transparência e na inovação — repete a narrativa de superioridade civilizatória que legitimou o expansionismo europeu, configurando, na governança de dados, um terreno de subordinação epistêmica.

Conforme buscamos reconstruir ao longo do capítulo, a governança da informação aparece como arranjo distribuído por infraestruturas, mercados e instâncias multilaterais, atravessado por assimetrias de poder que não se esgotam na figura do Estado. Esse quadro sustenta a leitura de “colonialismo de dados” como chave para entender fluxos, plataformas e regimes de visibilidade que reiteram dependências definindo quem aparece, quem conta e quem decide sobre padrões técnicos e normativos. Nesse ambiente, a circulação e a extração de dados assumem valor estratégico, deslocando as disputas regulatórias para arenas onde a

capacidade de processar, classificar e modular informação se converte em relações de poder. É nesse ponto, especificamente, que no Capítulo 3 a privacidade será tratada não como resíduo liberal universal, mas como dispositivo que emerge dentro dessa arquitetura planetária de controle e extração, já marcada por filtros geopolíticos e pela intermediação corporativa de infraestruturas, normas e narrativas.

Ao mesmo tempo, conforme buscamos trazer também, a inflexão neoliberal configura a vigilância como modelo de negócio e racionalidade de gestão, com imperativos de extração e predição que convertam experiência em insumo econômico. Essa racionalidade não apenas organiza plataformas e cadeias de valor como efetivamente informa o modo como problemas, riscos e responsabilidades são distribuídos — com ênfase crescente em métricas, desempenho e autogestão por parte de organizações e indivíduos, como veremos no Capítulo 3. Ao passo que avançamos, essa mesma matriz passa a ser observada no plano dos direitos, formulando a proteção da privacidade e dos dados pessoais em termos de gestão contínua de risco, documentação de conformidade e padronização procedimental, isto é, como uma "tecnologia de governo" acoplada às lógicas de mercado e às capacidades técnico-burocráticas descritas no capítulo anterior. Pela seção 2.3, ao mesmo tempo, procuramos sinalizar para um problema que orienta a virada analítica do capítulo seguinte, analisando a maneira pela qual políticas e regimes de privacidade operam num terreno já estruturado por assimetrias de acesso a dados e infraestruturas normativas. O Capítulo 3, portanto, investigará como a narrativa da privacidade em termos de direitos fundamentais é mobilizada e reconfigurada no interior dessa disputa, seja institucionalmente, seja subjetivamente, para produzir salvaguardas e, ao mesmo tempo, exigências de gestão do risco e auto-responsabilização. Em outras palavras, buscamos aqui sintetizar o movimento entre a cartografia das arquiteturas e racionalidades como condição de possibilidade do presente regime informacional, e a análise de como a privacidade se tornou um dispositivo central de sua governabilidade.

3. A privacidade como agenda política

A noção moderna de privacidade, em linhas gerais, emerge no interior do pensamento liberal como resposta à intrusão estatal e como fundamento da separação entre esferas pública e privada, articulando-se intimamente com a defesa da propriedade, da inviolabilidade e da liberdade individual (Arendt, 1958; Mill, 1859). No entanto, procuramos argumentar que essa concepção clássica se revelou insuficiente diante das transformações operadas pelas tecnologias de governo típicas da segunda metade do século XX, contexto no qual - procuraremos evidenciar - a privacidade perde gradativamente seu caráter de direito negativo e se converte em uma tecnologia de subjetivação e um mecanismo de gestão da vida.

Embora de início a tensão entre o ideal de liberdade individual e as exigências da racionalidade do Estado pareçam se acentuar na medida que crescem as intervenções de forma mais capilar na vida dos cidadãos, conforme tratamos no Capítulo 1, a privacidade, de fato, passa a operar como um dispositivo ambivalente. Ao mesmo tempo em que é mobilizada em torno da proteção à intimidade e a autonomia, legitima de igual maneira formas de classificação, vigilância e exclusão (Duncan, 2021; Lyon, 2001) que, em última instância, reforçam e fortalecem uma concepção securitária de gestão da vida social. Elemento chave da constituição histórica das democracias liberais como as conhecemos, pretendemos aqui compreender o lugar da privacidade no interior das tecnologias modernas de governo, tal como problematizar a naturalizada oposição entre a privacidade e a segurança, fortalecida principalmente a partir do contexto posterior ao 11 de setembro.

Essa ambivalência será central na forma como, ao longo do século XX, a privacidade é mobilizada em distintos marcos normativos, especialmente no pós-guerra, como valor fundante dos regimes democráticos, a despeito das recorrentes zonas de "exceção" (Bigo, 2014) nas quais a proteção da vida privada é suspensa "em nome da segurança". Assim, compreender a emergência da privacidade como problema político para os fins de nosso argumento exigirá, neste capítulo, mapear não só os elementos de sua representação moderna, mas sua imbricação estrutural com os regimes de visibilidade e controle no pano de fundo da presente pesquisa.

3.1 A emergência histórica da privacidade e da proteção de dados

Com frequência, no interlúdio das discussões sobre a expansão e distribuição das redes de vigilância, aparece a figura do *privacy advocate* (ou, do defensor da privacidade) como uma posição à frente da possibilidade de resistência e contenção do cenário trazido no Capítulo 1. Os defensores da privacidade - representados por ONGs, ativistas autônomos, instituições privadas etc. - são aqueles que vêm confrontando as transformações tecnopolíticas da captura dos dados pessoais. Apesar da maior atuação que parte destes grupos vem adquirindo - que se materializa, por exemplo, na adoção e atualização de normativas de proteção de dados ao redor do mundo -, parte dessa comunidade argumenta que a obstacularização constante da agenda da defesa da privacidade enfrenta, na forma do chamado "interesse público" (Bennet, 2006).

Parece haver, nesse sentido, sempre uma justificativa razoável para a captura de informações, principalmente em um contexto - como tratamos - de hegemonia cibernética. Os argumentos navegam entre a segurança nacional, a execução de políticas públicas e serviços de governo digital, eficiência do mercado, a proteção a fraudes, a produtividade nos espaços de trabalho, o monitoramento do consumo de energia para fins ambientais, enfim. Em resposta ao conjunto diverso de interesses *em prol* da legitimidade da vigilância nas sociedades contemporâneas, os defensores da privacidade dirão, em geral, que a sua proteção não é incompatível com a promoção da segurança e da eficiência, pelo contrário. Cada vez mais, o suposto paradoxo entre a privacidade e a vigilância vem sendo codificado em regimes normativos que parecem, a princípio, tentar equilibrar essa relação e estabelecer os limites de pervasividade de um sobre o outro. Nesse contexto, o conceito permanece incômodo no interior do campo dos estudos da vigilância, sendo por vezes criticado por seu excesso de individualismo (Gandy, 1993;) ou pela sua inadequação universalizante, incapaz de incorporar problemáticas provenientes de populações historicamente marginalizadas (Monahan, 2015; Gillion, 2001)

É, entretanto, evidente na literatura a dificuldade de conceitualização da privacidade, em termos de seu escopo, implicações e marcos de governança, e o forte tensionamento em relação a seu potencial explicativo - e, é claro, transformador - da ordem contemporânea. Nissenbaum (2010), Moore (2010), Cohen (2013) e Solove (2008) desenvolveram nas últimas décadas a tentativa de produzir um núcleo conceitual coerente e unificado em torno de

diferentes tipologias, normas e valores associados à proteção da privacidade e dos dados pessoais[17], em geral buscando enfatizar uma dimensão contextual de definição, que parte, portanto, de ações, ameaças e problemas diante que ora o indivíduo, ora o "espaço" da vida privada estariam confrontando. Mesmo a produção normativa, a nível internacional, tende a se debruçar de forma ambígua sobre os objetos que efetivamente constituem a privacidade, quais interesses estariam em jogo, como (e se) deveriam ser protegidos e valorizados. Se parte dessa literatura e experiência por vezes adota uma perspectiva quase que exclusivamente instrumental, mais recentemente, na medida em que concepções teóricas procuram impactar em dispositivos legais, se multiplicam as contribuições que procuram definir a privacidade como um *cluster* de valores.

A noção de "direito à privacidade" é popularizada em 1890 no contexto do artigo de Samuel Warren e Louis Brandeis, *The Right to Privacy,* considerado uma das mais relevantes reflexões da história do direito norte-americano. A princípio descrito pelos autores como o direito do indivíduo de *"determinar até que ponto seus pensamentos, sentimentos e emoções serão compartilhados com outros (...) fixando os limites da publicidade que lhes será atribuída"* (WARREN e BRANDEIS, 1890). Era necessário, nesse sentido, que se reconhecesse que a quando a vida privada - os hábitos, as ações, as relações - se torna publicamente disponível, poderá influenciar ou prejudicar "*o próprio cerne da personalidade de um indivíduo - sua estima de si mesmo"* (WARREN e BRANDEIS, 1890). Em um primeiro momento, portanto, o direito à privacidade constitui, para Warren e Brandeis, o direito do indivíduo de proteger nada mais do que sua reputação - sua integridade psicológica, na terminologia dos autores -, por meio do exercício do controle das informações de sua vida privada. Tal como "o direito de ser deixado em paz" (do inglês, *the right to be left alone*), que aparece ainda em 1879, mobilizado em termos do "*direito à imunidade completa"* (COOLEY, 1879), a defesa da reputação e da personalidade de Warren e Brandeis parece evocar um desenvolvimento natural e inexorável das sociedades modernas,

[17] A distinção entre o direito à privacidade e o direito à proteção de dados pessoais é essencial. O primeiro corresponde a uma liberdade negativa, isto é, ao direito de afastar-se do espaço público e preservar uma esfera privada, sendo condicionado pelos modelos de negócio e pelos avanços tecnológicos que podem fortalecê-lo ou restringi-lo. Já o segundo configura uma liberdade positiva, vinculada à autodeterminação informativa, pela qual o indivíduo exerce controle sobre o tratamento de suas informações, ainda que estas sejam públicas. No campo da governança da internet, a proteção de dados adquire destaque por conjugar autonomia individual e regulação das informações acessíveis publicamente. Para uma recuperação contextual da distinção entre os dois termos, ver Anexo I.

> A proteção da sociedade deve vir principalmente do reconhecimento dos direitos do indivíduo. Cada homem é responsável apenas por seus próprios atos e omissões. Se ele condena o que reprova, tendo em mãos uma arma equivalente à sua defesa, ele é responsável pelos resultados. Se ele resistir, a opinião pública se unirá a seu favor. Ele tem, então, tal arma? Acredita-se que o direito consuetudinário lhe fornece uma, **forjada no lento fogo dos séculos e, hoje, adequadamente temperada para sua mão**. O direito consuetudinário sempre reconheceu a casa de um homem como seu castelo, inexpugnável, muitas vezes, até mesmo para seus próprios oficiais envolvidos na execução de suas ordens. (WARREN e BRANDEIS, 1890, tradução e grifo nossos.)

No contexto da Constituição norte-americana, Warren e Brandeis situavam a privacidade dentro da tríade estabelecida pela Quinta Emenda - aquela que assume que nenhum indivíduo pode ser privado de sua liberdade, vida ou propriedade. Observa-se que, no final da década de 1880, os Estados Unidos vivenciavam um período em que o crescimento demográfico e a intensa urbanização resultavam em condições de superlotação nos espaços da vida social nas cidades, impactando significativamente a percepção da preservação da privacidade. Além disso, o fim da Guerra Civil impulsionara o desenvolvimento tecnológico, gerando inovações nas maneiras de publicização e acessibilidade à esfera da vida privada alheia: os telefones, o telégrafo, câmeras portáteis, dispositivos de gravação, etc. Associados a maior circulação de meios de comunicação impressos, circula a suposição de que os indivíduos estariam mais vulneráveis a terem publicamente expostas suas palavras e ações, sobretudo sem seu devido consentimento. *The Right to Privacy*, nesse sentido, resume um conjunto de preocupações de sua época sobre as crescentes ameaças - representadas por "dispositivos mecânicos" (Warren e Brandeis, 1890) - de coleta e disseminação de informações individuais.

Em um primeiro momento, consequentemente, o direito à privacidade corresponde àquele que poderá ser invocado para proteger o indivíduo contra tecnologias de invasão - pela imprensa ou por qualquer outro dispositivo moderno capaz de gravar ou reproduzir cenas ou sons (Warren e Brandeis, 1890). Há de se apontar, ainda, que o próprio Samuel Warren - filho da elite comercial de Boston, formado pela Escola de Direito da Universidade de Harvard - vivia a experiência de ter a vida de sua família exposta em colunas sociais do jornal local, ao mesmo tempo em que sua defesa da privacidade argumentaria que *"a imprensa está ultrapassando os limites óbvios da propriedade e da decência (...) para ocupar os indolentes, colunas são preenchidas com fofocas vazias, que só podem ser obtidas através da intrusão no círculo doméstico"* (WARREN e BRANDEIS, 1890). No interior do debate sobre a influência

da "jornalização" sobre a reputação de "homens públicos", o apelo à privacidade parecia constituir o discurso proeminente dos setores da sociedade que mais se percebiam como alvos. *"Se os jornais são úteis para derrubar tiranos, é apenas para estabelecer uma tirania própria. A imprensa exerce tirania sobre homens públicos, cartas, artes, o palco e até mesmo sobre a vida privada"* (COOPER, 1969), bradam contra a impertinência dos jornais do partido liberal inglês, cujos objetivos nada mais seriam do que *"a violação da paz pública, incitando os alvos à vingança e, talvez, ao derramamento de sangue*" (BLACKSTONE, 1966).

O reconhecimento constitucional do direito à privacidade, entretanto, é um fenômeno recente, na forma de um direito de escopo abrangente, para além da inviolabilidade da propriedade e da confidencialidade das comunicações. Em 1948 a Declaração Universal dos Direitos Humanos estabelece um direito geral à privacidade, assumindo que *"ninguém deve ser submetido a interferências arbitrárias em sua privacidade, família, lar ou correspondência, nem a ataques à sua honra e reputação"* (DUDH, 1949, grifo nosso). Dois anos depois, a Convenção Europeia dos Direitos Humanos incorpora o "respeito pela vida privada e familiar" que, posteriormente, seria reformulado no interior do Tribunal Europeu de Direitos Humanos na forma, apenas, do "respeito pela vida privada".

Algumas das mais famosas definições (WESTIN, 1967) de nosso conceito-chave giram em torno de experiências individuais da vida cotidiana, e sua relação e/ou grau de envolvimento com a esfera pública. Se, por exemplo, a *solidão* - o mais completo estado da privacidade - e a *intimidade* correspondem a estados de relativa separação ou reclusão, o indivíduo em estado de *anonimidade* ou *reserva* é ainda capaz de se preservar de identificação alheia, correspondendo a "aspectos dinâmicos da privacidade" relegados pelas relações interpessoais e o desejo pela "privacidade pública". Alan Westin (1967), ainda no registro do debate legalista de Warren e Brandeis, entende o espectro da privacidade como um que diz respeito a escolha e a possibilidade de compartilhar ou ocultar informações pessoais, limitando a comunicação a respeito de si quando em contato (amplo ou reduzido) com terceiros, se baseando na suposta "*necessidade de reter alguns aspectos de nós mesmos em relação aos outros, seja por serem* ***demasiado pessoais e sagrados****, ou por serem demasiado* ***vergonhosos e profanos*** *para serem expressos."* (WESTIN, 1967, p. 35, grifo nosso)

Considerações mais contemporâneas procuraram enfatizar a interface da preocupação com os valores associados à privacidade, é claro, no contexto da circulação de tecnologias computo-informacionais. Roger Clarke e Annita Allen apresentam, nesse sentido, categorias relacionais, à luz das diversas dimensões da vida social atravessadas pela "necessidade" da privacidade, dentre as quais ressaltamos a privacidade no âmbito da comunicação, a privacidade no âmbito dos dados pessoais e a privacidade no âmbito da experiência (CLARKE, 2016.). Enquanto as duas primeiras correspondem, de forma bastante intuitiva, a possibilidade dos indivíduos de se comunicar livres de monitoramento de terceiros e a possibilidade do indivíduo de exercer algum tipo de controle sobre seus dados pessoais, a terceira categoria, por sua vez, diz respeito à dimensão especialmente característica da privacidade no século XXI, aquela que diz respeito a todo conjunto de registros e armazenamento de dados exportados de interações *online*, acumulando quantidades massivas de experiência humana disponível para acesso e exploração (CLARKE, 2016; ZUBOFF, 2019) - na forma, é claro, daquilo que Shoshana Zuboff localiza no centro do chamado capitalismo de vigilância: o excedente comportamental. Apesar das eventuais manchetes apocalípticas anunciando o fim da privacidade na “Era Digital”, parte dessa literatura localiza o principal risco da falência do paradigma da privacidade não no desenvolvimento tecnológico - ou em sua interceptação pelo capital - mas na manutenção de um conceito, na base de toda sua estrutura normativa, que não dialoga efetivamente com o interesse público. Regan coloca

> Quando a privacidade é definida como um direito individual, a formulação de políticas passa a envolver um equilíbrio entre o direito individual à privacidade e um interesse ou direito concorrente. Em geral, o interesse concorrente é reconhecido como um interesse social. Por exemplo, o interesse da polícia na aplicação da lei, o interesse do governo na detecção de fraudes e o interesse de um empregador em garantir uma força de trabalho honesta são frequentemente discutidos e definidos como interesses sociais. Parte-se também do pressuposto de que o indivíduo possui uma participação nesses interesses coletivos. Como resultado, a privacidade tem estado em posição defensiva, cabendo àqueles que alegam uma violação de privacidade o ônus de provar que determinada atividade realmente invade a privacidade — e que o benefício social obtido com tal invasão é menos importante do que o dano individual sofrido. (REGAN, 1995, p. 40. Tradução nossa.)

Nessa direção, alguns autores propõem que o conceito de privacidade precisaria ser considerado da perspectiva das ameaças e riscos coletivos à sua violação social, reorganizando, inclusive, a própria fronteira tipicamente instituída entre a vida pública e a

vida privada. Essa problematização do conceito passaria pela interpretação da privacidade como um valor comum, público e coletivo, elevando a noção da privacidade para uma cuja defesa implica na proteção dos próprios sistemas democráticos. Ao mesmo tempo, a percepção do valor coletivo da privacidade procura enfatizar que, como consequência da distribuição das redes de coleta de informações, não haveria qualquer possibilidade de preservar ou garantir a privacidade de um indivíduo sem que o mesmo fosse feito para toda a população interceptada pelas mesmas redes.

Outra entre as propostas reformadoras do conceito da privacidade que ganha destaque contemporaneamente é a de Helen Nissenbaum. A autora concordará com a insuficiência das distinções liberais do "público" e do "privado", que ela localiza no centro da formulação normativa em torno da privacidade e da vigilância, a desenvolve um arcabouço de "integridade contextual" (NISSENBAUM, 2010) para responder a práticas informacionais típicas de nosso contexto.

Nissenbaum parte do pressuposto de que a preocupação central em torno do controle individual sobre a informação seria inadequada para dar conta da complexidade das demandas contemporâneas do direito à privacidade, argumentando que não se trataria simplesmente de restringir os fluxos de informação, mas de garantir - pelo arcabouço da integridade contextual - que os fluxos ocorram de forma adequada para distintos contextos sociais. A proposta, portanto, ajusta a regulação dos fluxos em torno das normas sociais e legais que governam as informações pessoais em diferentes situações - nos setores da educação, da saúde, da segurança, etc. - e diferentes ambientes culturais e históricos, para melhor compreender de que forma determinadas relações e interesses, sempre contextuais, poderiam ser equilibrados de forma a não privilegiar determinados grupos de interesse. Para a autora

> Por mais que possamos nos sentir inquietos diante de tecnologias que **reduzem nosso controle sobre as informações pessoais**, ainda mais preocupantes são aquelas que **desconsideram normas sociais consolidadas**, pois, ao fazê-lo, ameaçam desestabilizar o próprio tecido da vida social. É certo que **nem todos os sistemas que alteram o fluxo de informações** são motivo de alarme: há casos evidentes em que **novos dispositivos e sistemas informacionais** atendem melhor aos **valores, fins e propósitos sociais e contextuais** do que aqueles que já temos (por exemplo, ao promover o desenvolvimento intelectual, a saúde, o bem-estar e uma democracia vibrante). Nesses casos, o sistema em questão geralmente é — e deve ser — **aceito, até mesmo celebrado**.Temos, sim, um **direito à privacidade**, mas ele **não é um**

> **direito de controlar informações pessoais**, nem um direito de restringir o acesso a essas informações. Em vez disso, trata-se de um **direito de viver em um mundo no qual nossas expectativas sobre o fluxo das informações pessoais sejam, em grande parte, respeitadas**. (NISSENBAUM, 2010, p. 223. Grifos nossos. Tradução nossa.)

É portanto pela busca das *normas enraizadas* em torno da privacidade e da proteção de dados, que estariam sob risco diante do potencial intrusivo das novas tecnologias. A origem da indignação social sobre a intrusão, aqui, reside em uma ruptura em relação àquilo que as pessoas entendem como o uso "normal" de suas informações e dados pessoais. O fato de que, entretanto, a autora procura identificar *a norma correta* para a privacidade, a norma para governar sobre todas as outras, peca não apenas pelo conservadorismo intrínseco (Rile, 2019), inclusive anunciado pela própria autora, mas também com a impossibilidade de mapear aquelas intrusões que operam sem perturbar os limiares da perturbação da "moral" pública, tampouco a serviço de quais interesses as expectativas de determinadas normas são ou não são desestabilizadas.

Além de identificar normas ameaçadas ou denunciar violações pontuais, importará aqui, de igual maneira, interrogar os próprios mecanismos pelos quais certos arranjos normativos se estabilizam como evidências incontestáveis do que deve ser protegido. A naturalização da privacidade como valor universal implicaria, possivelmente, no risco de ocultamento dos processos pelos quais ela é continuamente produzida, reinscrita e instrumentalizada em contextos específicos. Em vez de operar como um limite ao arbítrio, a categoria serve muitas vezes como ferramenta de organização de relações sociais desiguais, definindo quem pode controlar a circulação de informações. Trata-se, assim, de deslocar o foco da norma ameaçada para os regimes que, sob o signo da privacidade, modulam expectativas, distribuem privilégios e legitimam dispositivos de vigilância como operações neutras.

Neocleous (2002) e Henry (2013), nessa direção, procuram enfatizar as contradições histórico-políticas do conceito, erguido principalmente sobre a distinção entre o público e o privado. Recuperando a origem da concepção da privacidade como virtude política no contexto de desintegração de espaços tipicamente pré-modernos e consolidação da "vida privada" e da "vida pública". Estaria, portanto, na emergência do Estado Moderno a certidão de nascimento do valor da privacidade, ao mesmo tempo em que se estruturam as próprias instituições modernas em cujo cerne estaria a necessidade permanente de coleta de

informação (Neocleous, 2002). Não seria nada surpreendente, portanto, a insuficiência sistemática de iniciativas de defesa da privacidade no interior das democracias liberais, dado que - dessa perspectiva - a violação da prerrogativa estatal à informação e a confidencialidade, implicaria na violação da própria razão de Estado, fundada sobre uma máquina de produção e gestão do segredo, uma de ocultamento deliberado da informação sob o manto da segurança (Neocleous, 2002). O suposto tensionamento entre a transparência e a confidencialidade, nesse sentido, seria parte estrutural da governamentalidade moderna, permitindo ao Estado determinar zonas de opacidade alinhadas a narrativas em prol do interesse público e da proteção da ordem. A defesa liberal da transparência e da privacidade seria portanto confrontada sob acusação de gestoras simbólicas da crítica do poder do segredo que, em última instância, permaneceria tecnicamente racionalizado, mas intacto.

Mais do que isso, os autores problematizam o discurso liberal do direito à privacidade como um de despolitização dos conflitos sociais subjacentes, ignorando o papel da privacidade na manutenção de relações de exploração no espaço doméstico, familiar e do consumo - a privacidade, dessa perspectiva, contribui para tornar certas formas de poder invisíveis. Articulando o campo semântico entre privacidade, confidencialidade e idiotia (do inglês, *privacy, secrecy* e *idiocy*), Neocleous sugere que a celebração da privacidade pode resultar numa forma de idiotização política e apatia funcional à reprodução da ordem:

> What privacy manifestly fails to do as an organizing concept is provide any grounds for collective resistance (...) This is precisely what capital and the state want us to do: they want us to remain rooted in the legacy of eighteenth century Robinsonades, to choose the life of what the Greeks thought of as the idiot - a life of "one's own" instead of a life in collective pursuit of a rational society (...) in other words, they want us to be idiots. In fetishising privacy we therefore run the risk of shackling our ability to combat the state collectively. (NEOCLEOUS, 2002, p. 107)

Em direção semelhante, Henry (2013) propõe que a privacidade seja compreendida não como uma liberdade a ser protegida ou regulada, mas como um objeto político permanentemente administrado, ou seja, um campo de produção normativa voltado à pacificação da vida social. Recusando a ideia de que a regulação da privacidade limitaria abusos do Estado e do mercado sobre os indivíduos, argumenta que a crescente onda de políticas de governança da privacidade pretendem, no limite, mediar o conflito entre capital, Estado e sociedade civil, canalizando dissidências para suas formas mais administráveis.

Mantida sob um estado de “crise permanente”, a privacidade seria o objeto por excelência da regulação constante, permanente e flexível - aparecendo aqui, portanto, como uma categoria produtiva, organizadora de condutas, distribuidoras de responsabilidades e legitimadora de intervenções técnicas e jurídicas em nome do “risco”, da “segurança” ou do “interesse público. Instrumentos tais como trataremos mais adiante - como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) ou a Lei Geral de Proteção de Dados (LGPD), por exemplo - seriam efetivamente instrumentos performativos, produtores de sujeitos privados e dos riscos a serem governados.

Ao tensionar a gramática liberal que ancora as promessas de proteção da privacidade, as análises de Henry e Neocleous deslocam o foco da denúncia da vigilância para os próprios mecanismos que tornam sua gestão possível, revelando como a privacidade opera não como limite ao poder, mas como linguagem funcional à sua reorganização. Essa chave de leitura convida a ultrapassar a dicotomia entre a privacidade e a vigilância, permitindo reconhecer a primeira como superfície estratégica de recomposição da autoridade regulatória diante das transformações tecnológicas e econômicas do capitalismo digital. Nesse deslocamento, abre-se espaço para compreender também as transformações ontológicas que essa normatização produz nos regimes de legibilidade e inteligibilidade do sujeito, da informação e da vida social. Trata-se, portanto, de examinar como a privacidade se reconfigura como tecnologia de inscrição e diferenciação, simultaneamente jurídica, técnica e social, tornando-se peça-chave na arquitetura de um novo regime epistêmico de governamentalidade. É justamente nesse terreno que se insere a contribuição de Julie Cohen (2013), ao explorar os efeitos da informatização sobre as formas pelas quais o espaço privado é capturado, rearticulado e governado sob lógicas infraestruturais.

A partir dos anos 1990, especialmente com a ascensão da Internet comercial e das plataformas de processamento de dados em larga escala, intensifica-se o que a autora chama de “reconfiguração da esfera privada” sob condições informacionais. Nesse cenário, a privacidade deixa de ser um atributo a ser protegido e passa a ser uma condição a ser constantemente negociada, reconfigurada e, muitas vezes, sacrificada. Mais do que um direito subjetivo individual, a privacidade parece então se afirmar, ao longo do século XX, como um dispositivo normativo de múltiplas camadas de significação. Sobretudo em sua formulação moderna, deve ser compreendida como parte integrante da arquitetura liberal da segurança como tecnologia de governo: opera como técnica da gestão da população, estabelecendo

zonas de visibilidade e invisibilidade que regulam a circulação da informação e os próprios limiares do que deverá ser governado. Reorganizando os modos pelos quais o espaço privado é representado, medido e eventualmente exposto, moldando o que se torna rastreável, quantificável e controlável, a privacidade - como direito e como *dispositivo* – encontra novo fôlego no contexto da informatização da economia e dos processos sociais.

A ascensão de modelos de negócios centrados na extração de dados pessoais, conforme trouxemos no Capítulo 2, inscreve a privacidade em uma lógica de mercado que transforma a autonomia em mercadoria e o consentimento em moeda regulatória, conduzindo a um processo não apenas de erosão do direito à privacidade, mas sua reinscrição funcional em um regime neoliberal de subjetivação, onde o indivíduo se torna responsável por sua própria proteção informacional em um ecossistema assimétrico e opaco, como trataremos mais adiante. É a partir dessas inflexões que a privacidade se torna objeto de disputas regulatórias em nível internacional.

Ao mesmo tempo em que regimes jurídicos como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) se propõem a reafirmar a autodeterminação informativa como direito fundamental, modelos regulatórios centrados no consentimento e na gestão de riscos - como o norte-americano e, em grande medida, o brasileiro - acabam por reduzir a privacidade à condição de produto transacionável, adaptável às necessidades do mercado e das infraestruturas digitais dominadas por corporações transnacionais (BROWNSWORD, 2019; BENNETT & RAAB, 2006). Como trataremos nas seções seguintes, a governança global da privacidade se estrutura, assim, sobre relações de dependência regulatória e imposição de lógicas neoliberais de responsabilização individual em nome da liberdade de escolha. A emergência histórica da privacidade, portanto, longe de esgotar-se em sua formulação clássica, atualiza seus termos em torno da reconfiguração contemporânea de seus sentidos – ao mesmo tempo instrumento de liberdade e de controle.

3.2 A governança global da privacidade: instituições, regimes e assimetrias normativas

Se na seção anterior procuramos tratar da emergência da privacidade como uma noção tensionada, é precisamente no campo da regulação internacional que se desdobra uma arena de disputas sobre sua operacionalização normativa. A aparente universalização do direito à privacidade não se deu de forma homogênea, tampouco resultou em um regime coeso; ao

contrário, o que se observa é a formação de um campo dinâmico e fragmentado, onde distintas tradições jurídicas, interesses geopolíticos e tecnologias de governo disputam a autoridade regulatória sobre o tratamento e a circulação de dados. Neste cenário, os regimes internacionais de proteção de dados e privacidade operam, por um lado, como tentativas de coordenação normativa, e por outro como artefatos técnicos que performam distintos modelos de governança. A análise que segue procurou articular a diversidade desses regimes com as disputas em torno da sua interoperabilidade e com os efeitos políticos da fragmentação normativa, recuperando os principais instrumentos regulatórios globais e suas procedências.

A constituição de regimes internacionais de proteção da privacidade e dos dados pessoais se inscreveu no interior de uma racionalidade política que busca estabilizar padrões normativos mínimos frente à crescente circulação transfronteiriça de informações. No entanto, como sugere Colin J. Bennett (2008), esse processo não se dá de forma unívoca, mas como consequência de múltiplas trajetórias nacionais que convergem e se friccionam em dimensão global, interconectadas inevitavelmente aos processos que marcam a evolução do debate da governança da Internet. Bennett (2008) demonstra que embora os regimes nacionais de privacidade tenham emergido a partir de pressões domésticas específicas, foram progressivamente afetados pela necessidade de interoperabilidade regulatória diante de fluxos globais de informação e da emergência de uma economia política digital transnacional. Mais do que uma homogeneização normativa, o que se observa é uma governança por instrumentos — como definido pelo autor — que opera por meio da difusão seletiva de modelos, *standards* técnicos e esquemas de auto ou co-regulação.

O resultado desse processo (Bennet, 2008) não é a universalização de uma norma, mas a construção de uma matriz de interoperabilidade parcial e performática, em que mecanismos, cláusulas contratuais padrão e certificações tentam compatibilizar diferentes ordenamentos sem suprimir suas diferenças estruturais. Essa forma de governança por instrumentos produz, por um lado, um mínimo denominador comum regulatório, necessário ao funcionamento das cadeias globais de valor da informação; por outro, consolida assimetrias de poder entre regimes emissores e receptores de dados. A própria Comissão Europeia, ao emitir decisões de adequação — como nos casos[18] do Japão, do Reino Unido ou do Uruguai — atua como

[18] Em 2019, a Comissão Europeia adotou uma decisão de adequação para o Japão, reconhecendo que o país garantia nível de proteção de dados pessoais essencialmente equivalente ao europeu. Esse foi o primeiro caso recíproco: o Japão também adotou regras complementares para alinhar suas práticas ao GDPR, especialmente no que diz respeito a categorias sensíveis de dados e direitos de acesso. Esse arranjo foi apresentado pela Comissão

agente de normatização, deslocando o eixo do debate sobre soberania e privacidade para uma arena transnacional de regulação majoritariamente econômica. Essa dinâmica se torna ainda mais complexa diante das crescentes tensões entre regimes de proteção e regimes de segurança.

O *Privacy Shield* (revogado em 2020 pela decisão da Corte de Justiça da União Europeia) e os acordos de intercâmbio de dados entre Estados Unidos e União Europeia exemplificam, de igual maneira, como o campo da privacidade é também o campo da exceção, no interior dos quais a segurança nacional pode suspender garantias de direitos sob o argumento da "necessidade proporcional". O que emerge, portanto, é o efeito de regimes concorrentes, em que a interoperabilidade é menos um consenso jurídico que uma condição técnica e econômica para a operação do quadro que procuramos apresentar no Capítulo 2. A fragmentação normativa, longe de ser um obstáculo, pode ser interpretada como uma tecnologia que permite o ajuste flexível da proteção de dados às prioridades geoeconômicas e securitárias de determinados atores, ao mesmo tempo em que fornece um léxico universal de direitos apto a legitimar determinadas práticas.

Tradicionalmente, o ponto de partida em termos da internacionalização dos princípios fundamentais para proteção da privacidade e proteção de dados é localizado nas Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) sobre Privacidade e Fluxos Transfronteiriços de Dados Pessoais (1980). As diretrizes procuraram estabelecer os princípios fundamentais para proteção de dados pessoais - incluindo a limitação da coleta, qualidade dos dados, transparência, segurança e direitos dos titulares, constituindo uma base originária para diversas legislações nacionais (OCDE, 2013). Rapidamente, entretanto, uma série de interpretações oscilantes sobre conceitos como "dados pessoais" e "consentimento" apresentaram obstáculos práticos para sua aplicação efetiva (Greenleaf, 2020; Bennet, 1992), principalmente no desencontro entre a facilitação do comércio digital e a proteção de dados.

---

como a maior área de livre fluxo de dados do mundo, cobrindo tanto a União Europeia quanto o Japão. após o Brexit, em 2021, a Comissão Europeia aprovou uma decisão de adequação permitindo que dados pessoais continuassem a circular do EEE para o Reino Unido sem necessidade de salvaguardas adicionais. O reconhecimento considerou a legislação britânica — basicamente herdada do GDPR durante o processo de saída — como equivalente ao regime europeu. O Uruguai, por sua vez, foi o primeiro país da América Latina a receber uma decisão de adequação, ainda em 2012, com base na sua Lei n.º 18.331/2008, que instituiu um regime de proteção de dados inspirado nos padrões europeus. Esse reconhecimento permitiu que transferências de dados da UE para o Uruguai ocorressem livremente, sem cláusulas contratuais adicionais. O caso foi simbólico ao demonstrar a capacidade de um país latino-americano alinhar-se com as exigências normativas europeias, integrando-se a fluxos globais de dados.

Questões relativas ao equilíbrio entre a interoperabilidade (implicada na livre circulação de dados transfronteiriços, essenciais em cadeias logísticas globais e serviços digitais) e o princípio de soberania digital (UNCTAD, 2021), às pressões por harmonização regulatória, por parte dos organismos multilaterais e pelas grandes corporações digitais interessadas na redução de custos e incertezas jurídicas, por um lado, e a subordinação de direitos e especificidades locais, por outro (UNHRC, 2021) e aos conflitos entre modelos de negócios digitais e princípios de autonomia informacional e consentimento livre e informado (OHCHR, 2022) representam alguns dos termos gerais do debate que se coloca diante das diretrizes trazidas pela OCDE, e que permanecerão na mesa na medida em que novos marcos normativos levantados ao redor do planeta.

As diretrizes da OCDE desde sua origem, não operam como barreira regulatória, mas como infraestrutura de circulação, conectando o direito à privacidade ao imperativo econômico dos fluxos informacionais. No texto original de 1980, já se afirmava a necessidade de *"facilitar os fluxos de dados pessoais através das fronteiras, evitando ao mesmo tempo abusos que possam violar a privacidade e as liberdades individuais"* (OCDE, 1980, p. 7. Tradução nossa.). Essa formulação inaugura um padrão de normatividade orientado à sua condicionalidade, admitindo a coleta e transferência de dados pessoais desde que acompanhadas de um conjunto mínimo de princípios, nomeadamente: limitação, qualidade, propósito, limitação, segurança, transparência, participação individual e *accountability.* Ao definir esses princípios em linguagem genérica, as Diretrizes visaram criar um consenso entre países com tradições jurídicas distintas, permitindo que a proteção de dados fosse reconhecida, naquele contexto, como condição da confiança necessária ao comércio informacional-internacional.

O princípio da participação individual - não tão distinto da prerrogativa do consentimento -, tal como enunciado pela OCDE em 1980, estabelecia que o titular, ou, o sujeito dos dados deve ter a possibilidade de obter do controlador a confirmação da existência de dados a seu respeito, ter acesso a esses dados em prazo razoável, em formato inteligível e a custos não excessivos, bem como o direito de contestar e exigir retificação ou apagamento em caso de descumprimento (OCDE, 1980, p. 14). Essa formulação, reforçada em 2013, pretendia projetar a privacidade como um regime de transparência informacional, no qual o indivíduo é concebido como parte ativa no controle de seus próprios dados. No entanto, ao condicionar a efetividade desse direito a critérios de razoabilidade, custo e viabilidade

técnica, o princípio é deslocado para um campo de ponderação contínua, em que o exercício da participação individual é vinculado à infraestrutura organizacional. Como observa Bygrave (2015), a proteção acaba por ser um mecanismo que convida o indivíduo a participar ativamente de um regime de autogoverno informacional, cuja materialização depende da capacidade técnica e administrativa das organizações. Em parte, a literatura tem chamado atenção para a dualidade desse princípio. Se, por um lado, ele inaugura um direito fundamental de acesso e retificação — mais tarde consolidado em legislações como a Diretiva Europeia de 1995 e o GDPR (art. 15 e seguintes) , como veremos —, por outro, reforça uma racionalidade responsabilização do sujeito e exercício permanente de monitoramento sobre si mesmo (Passetti et al., 2020).

O princípio da transparência, a partir de lógica semelhante, estabelece que deve haver uma política geral de transparência em relação a práticas de coleta e uso de dados, de modo que *"there should be a general policy of openness about developments, practices and policies with respect to personal data"* (OCDE, 1980, p. 15). Essa formulação, retomada em 2013, explicita que indivíduos devem ter condições de conhecer quais dados são coletados e com quais propósitos, além de quem exerce controle sobre eles. Num primeiro olhar, o princípio parece consagrar uma racionalidade democrática da informação, se materializando entretanto em aportes técnicos e políticas de privacidade cujo acesso não se traduz automaticamente em compreensão efetiva. Bennett e Raab (2020, p. 112) enfatizam que a transparência, embora normativamente celebrada, muitas vezes resulta em um acúmulo de notificações formais que deslocam a responsabilidade de avaliação para os sujeitos, reiterando o problema da *"overload of information"* que elimina qualquer capacidade real de agência. Embora na forma de controle social, a transparência, dessa perspectiva, reforça a centralidade dos intermediários técnicos e a assimetria entre titulares e organizações.

O princípio da accountability, por sua vez, à época um dos mais inovadores das Diretrizes da OCDE, ao exigir que *"a data controller should be accountable for complying with measures which give effect to the principles stated above*" (OCDE, 1980, p. 15), consagra a ideia de que não basta enunciar garantias formais, sendo necessário atribuir deveres contínuos de diligência às organizações. Em 2013, a atualização reforçou esse eixo ao vincular *accountability* a práticas de gestão de risco e a mecanismos de auditoria e certificação. Kuner (2015, p. 31) observa que esse deslocamento foi fundamental para a posterior adoção, pelo GDPR, da lógica de "demonstrar conformidade", deslocando a

privacidade para um campo de *compliance*. De acordo com Bygrave (2015, p. 53), *accountability* aqui funcionará como um ponto de virada, conectando princípios substantivos a práticas organizacionais e métricas de performance.

A revisão de 2013 das Diretrizes, em síntese, reforçará esse viés. No preâmbulo, a OCDE afirmava que o objetivo era "*supporting the free flow of information while strengthening privacy protection"* (OCDE, 2013, p. 3), estabelecendo de forma explícita que a privacidade deveria ser instrumentalizada como fundamento da mobilidade global dos dados. São, ainda, introduzidos novos elementos, como o princípio do *risk management*, o foco em *security breach notification* e uma renovada ênfase em *accountability*. Bennett e Raab (2020, p. 113) dialoga com essa leitura ao afirmar que *"the OECD principles have been less a bill of rights for data subjects than a charter of responsibilities for organizations",* explicitando a inversão de foco da titularidade de direitos para a *accountability* das empresas. A chamada *soft law* nesse contexto passa a constituir um regime de governamentalidade no qual a circulação é protegida justamente porque a proteção é reconfigurada como gestão e auditoria do risco e da performance, à luz da necessidade de manutenção dos fluxos internacionais de informação.

Na esteira da OCDE, a Convenção 108 do Conselho da Europa (1981) aparece como o primeiro tratado vinculante internacional para proteção de dados pessoais, atualizada em 2018. Tipicamente organizado em torno de discursos em prol do fortalecimento da democracia e dos direitos humanos, o Conselho da Europa se volta ao tema da privacidade ainda na década de 1960, estabelecendo um comitê de boas práticas para proteção da privacidade com a difusão do uso de tecnologias informacionais (Bennet, 2006). A Convenção 108 - ou, Convenção para a Proteção das Pessoas Relativamente ao Tratamento de Dados de Carácter Pessoal - é resultado de duas resoluções anteriores, produzidas no interior do Comitê ao longo dos anos 1970, nomeadamente a Resolução 74 sobre a proteção dos indivíduos diante de bancos de dados digitais no setor público e a Resolução 73 sobre a proteção dos indivíduos diante de bancos de dados digitais no setor privado. Até 2001, a maior parte dos países membros era signatário da Convenção, e 25 deles tinham a ratificado. Sendo a primeira de seu tipo, a Convenção 108 operou como um template (Bennet, 2006) para legislação de proteção de dados ao redor do mundo, estimulando o entendimento que informações pessoais deveriam ser obtidas via processos legais, armazenadas para propósitos legítimos, adequados e relevantes em relação aos propósitos para seu armazenamento e

preservadas de forma a não permitir a identificação dos titulares por mais tempo do que aquele necessário e compatível com seu propósito.

Ao mesmo tempo, em seu Artigo oitavo, a Convenção estabelece a prerrogativa para indivíduos solicitarem informações sobre seus próprios dados, terem acesso aos dados coletados e armazenados, o direito de corrigi-los ou apagá-los e incorpora, de maneira inédita, a noção de que determinadas categorias de dados pessoais não deveriam ser tratados a menos que submetidos a salvaguardas jurídicas nacionais. Parte central da Convenção - similar as Diretrizes da OCDE antes dela, e de marcos regulatórios posteriores - reside, no Artigo 12, em orientações para fluxos transnacionais de dados, pretendendo garantir um grau equivalente e equilibrado de proteção para todas as partes a fim de promover a livre circulação de informações. Esse objetivo, entretanto, não foi cumprido de forma bem-sucedida pela Convenção, rapidamente se tornando claro no contexto da União Europeia que desalinhamentos no tratamento e proteção de dados implicariam em obstruções graves para o pleno funcionamento do Mercado Comum Europeu.

Essa inflexão, para Bennet e Raab (2006; 1997), marca o deslocamento da proteção de dados - do ponto de vista do paradigma europeu - da proteção de direitos humanos para um princípio fundamental da operação do comércio internacional, na forma da Diretiva 95[46 sobre a proteção de indivíduos com relação ao processamento de dados e à livre circulação desses dados (UE, 1995). De início interpretada como excessivamente restritiva (Bennet e Raab, 1997; Simitis, 1995), a Diretiva é fortemente influenciada pelo setor privado, tendo sido revisada em 1992 para se adequar às expressas quanto à liberdade de circulação. Bennet (2006) resume

> (...) o conteúdo essencial da Diretiva pode ser compreendido como o resultado de compromissos negociados entre uma variedade de atores públicos e privados. À medida que a necessidade de proteção de dados passou a ser sentida de forma mais ampla na maioria das organizações públicas e privadas, começou a emergir uma rede mais extensa, fragmentada e complexa, composta por especialistas nos problemas específicos de proteção de dados de seus respectivos setores industriais ou áreas governamentais. (...) A European Direct Marketing Association, por exemplo, gastou milhões de dólares em lobby, principalmente contra a opção do "consentimento positivo" presente no rascunho de 1990. Interesses norte-americanos, especialmente nos setores de marketing direto e de informações de crédito, também encontraram aliados naturais entre seus homólogos europeus e ficaram satisfeitos em oferecer apoio político e financeiro para fortalecer esses esforços de lobby. (BENNET, 2006, p. 524. Tradução nossa.)

A compreensão compartilhada, à época, principalmente no contexto europeu, era de que uma legislação de proteção robusta não seria, de nenhuma maneira, incompatível com a livre circulação - pelo contrário, deveriam tratar-se de valores complementares em torno da percepção da centralidade da informação para o mercado comum europeu. Diferentemente, ainda, da Convenção que a precedeu, a Diretiva passa a incluir especificações quanto à natureza das autoridades nacionais para o tratamento de dados, as quais deveriam ser dotadas de capacidade de intervenção e investigação. Para o universo extra-europeu o avanço nas negociações para adoção da Diretiva passaram a representar fonte de preocupação, sobretudo nos termos estipulados pelo Artigo 25, que determinava que os estados-membros poderiam transferir dados para um ator externo apenas se o país em questão for capaz de garantir graus de proteção "adequados" (Simitis, 1995; Bennet e Raab, 1995). Na ocasião de inadequação, salvo exceções, o estado-membro em questão teria a prerrogativa de tomar as medidas necessárias para prevenir qualquer transferência de dados para o destinatário. Nesse contexto, algumas das preocupações levantadas giravam em torno da possibilidade de que os julgamentos de adequação estivessem sujeitos às variações dos processos internos do continente europeu, podendo ter pouco ou nenhuma relação com prerrogativas de proteção de dados e privacidade.

A adoção da Convenção permaneceu restrita e limitada, principalmente à luz da adoção, em 2016, do Regulamento Geral de Proteção de Dados (GDPR), ampliando significativamente os direitos dos titulares e impondo obrigações mais rigorosas e extraterritoriais para controladores, posicionando-se como o "padrão de ouro global" para governança de dados e para garantia de *fluxos seguros* de informações. Por outro lado, no mesmo contexto, a região do Pacífico opta por privilegiar a autorregulação e a cooperação público-privada, fortemente focada na facilitação do comércio digital (APEC, 2015) e se diferenciando substancialmente do paradigma europeu - enquanto, por sua vez, blocos como o Mercosul e a ASEAN avançaram aos poucos na adoção de regimes próprios, no interlúdio entre a fragmentação e os esforços pela harmonização, em âmbito cada vez mais global.

Em face de parte do debate descrito até então, e a supostamente compartilhada percepção da possibilidade frágil de harmonização regulatória, parte da solução é deslocada para instituições de certificação e *compliance*, enfatizando uma dimensão da proteção da

privacidade em termos técnicos de “gestão de qualidade", ao lado das demais normas reunidas pela Organização Internacional para Padronização (no inglês, ISO). Nesse contexto, em um primeiro momento, uma iniciativa liderada pelo Comitê Europeu de Normalização (CEN) propõe um padrão de proteção de dados capaz de estabelecer o passo-a-passo operacional a ser implementado por qualquer organização a fim de se adequar a legislações pertinentes - especificamente à Diretiva europeia vigente. Esse esforço é consolidado na forma da Iniciativa sobre a Padronização da Privacidade na Europa (IPSE), que defendiam a internacionalização de um modelo como amplamente vantajosa em relação a modelos nacionais em co-existência e eventual confronto:

> It would attract attention and international certification efforts from different national standards bodies. It would give business outside Europe a more reliable and consistent method by which to demonstrate their conformity to international data protection standards. (...) Required registration to a standard would oblige independent and regular auditing, would provide a greater certainty tat “adequate” data protection is being practised by the receiving organization, wherever it is located. This does, of course, require concomitant efforts to harmonize systems of conformity and certification. At the end of the day, bilateral and multilateral mutual recognition agreements would also have to be negotiated to ensure that domestic conformity programmes are commonly respected (BENNET, 2006, p. 159)

Gradativamente, portanto, a proteção da privacidade à nível internacional se aproximava de uma questão tratada em termos comerciais, o que inevitavelmente levou a integração da Organização Internacional do Comércio (OMC) no interior do debate regulatório influenciando, privilegiando os termos da discussão iniciativas de proteção de dados centradas na segurança da livre circulação. Criticada principalmente pelas autoridades norte-americanas em termos de beneficiar o ambiente de negócios da União Europeia e de obstruir o fluxo de dados entre países, a Diretiva passa a ser alvo de acusações de violação às normas da OMC.

Essa tensão em torno da compatibilidade entre regras de proteção de dados e compromissos comerciais multilaterais não permaneceu restrita ao embate dos anos 1990. Ao contrário, ela antecipou dilemas que se tornariam centrais nas décadas seguintes: como compatibilizar a promessa de garantias individuais com a demanda por circulação irrestrita de informações em escala global. O debate em torno da Diretiva de 1995, nesse sentido, inaugura uma disputa mais ampla sobre legitimidade regulatória, em que se confrontaram a linguagem do comércio internacional e a linguagem dos direitos fundamentais. À medida que

a economia digital expandia seu alcance, esse conflito se traduziu em arranjos cada vez mais sofisticados de equivalência normativa, nos quais a União Europeia buscou afirmar sua posição de potência regulatória enquanto respondia a pressões externas de governos e empresas transnacionais. É nesse deslocamento, da crítica dirigida à Diretiva para a consolidação do GDPR, que a questão da interoperabilidade normativa ganha relevância e passa a organizar o campo da proteção de dados e da privacidade em termos de convergência seletiva e disputas de soberania regulatória.

A experiência norte-americana ilustra de maneira paradigmática a fragmentação setorial e a prevalência de uma gramática do consumo na proteção de dados e da privacidade. A Health Insurance Portability and Accountability Act (HIPAA, 1996) instituiu um regime robusto para informações de saúde, mas já no seu próprio texto consagra exceções amplas. O §164.512 autoriza usos e divulgações de dados *"for public health activities, law enforcement purposes, and research under certain conditions"*, de modo que a privacidade do sujeito titular é reconhecida, mas imediatamente relativizada em nome da segurança pública. Essa estrutura confirma o caráter funcional do arranjo estadunidense, inserindo a privacidade como interesse a ser equilibrado frente a outras finalidades institucionais, reiterando a centralidade de uma governamentalidade do risco. A Children's Online Privacy Protection Act (COPPA, 1998) na mesma direção, ao impor consentimento verificável dos pais para a coleta de dados de menores de 13 anos, estabelece que *"it is unlawful for an operator of a website directed to children to collect personal information from a child in a manner inconsistent with the regulations prescribed."* (§6502(b)(1)(A)) A ênfase no consentimento parental projeta a proteção como responsabilidade do indivíduo (neste caso, na instituição familiar família), e não como limitação estruturante à exploração comercial dos dados (sensíveis) dos titulares. Como nota Solove (2013), trata-se de mais um exemplo da "ilusão do autogerenciamento da privacidade", em que se presume que sujeitos consigam compreender e administrar riscos em contextos de extrema assimetria de informação.

No setor financeiro, a Gramm-Leach-Bliley Act (GLBA, 1999) institui mecanismos de notificação e veto limitado, prevendo no §6802(b) que instituições financeiras *"may not disclose nonpublic personal information to a nonaffiliated third party unless the consumer is given notice and an opportunity to opt out."* Aqui, novamente, a proteção se realiza como prerrogativa de *opt-out*, exigindo que o consumidor exerça ativamente seu direito para impedir práticas de compartilhamento. A terminologia da lei é reveladora: não se proíbe o

tratamento, mas se transfere ao titular o ônus de rejeitar, em vez de garantir um direito inalienável. A crítica de Schwartz (2011) é precisa, ressaltando também que o referido modelo tende a privilegiar o fluxo econômico e a transformar a privacidade em objeto de escolha de mercado. Esse tripé — HIPAA, COPPA e GLBA — aponta para a existência de um padrão regulatório em que a privacidade é distribuída em legislações setoriais, acionada em termos de exceções funcionais e operacionalizada pelo consentimento ou pelo veto individual. A privatização da regulação, reforçada pela expansão de políticas internas, selos e certificações, reforça a projeção da privacidade como campo de *compliance* corporativo, deslocando o eixo da proteção para um arranjo que, em sua funcionalidade, converge com outros modelos globais, ainda que sob os termos particulares do neoliberalismo norte-americano.

A questão da interoperabilidade normativa emerge como um dos eixos mais complexos de nosso debate. Se por um lado a difusão do Regulamento Geral de Proteção de Dados (GDPR) europeu consolidou princípios comuns — como limitação de finalidade, minimização de dados e accountability —, por outro, sua aplicação transfronteiriça exigia negociações constantes e ajustes procedimentais. Não se trata de reconhecer diferentes tradições jurídicas, mas de lidar com uma "convergência imperfeita" (Kuner, 2020), em que arranjos locais incorporam seletivamente os princípios europeus sem abrir mão de especificidades normativas ou interesses estratégicos. O caso mais emblemático desse tensionamento permanece o *Schrems II*, em 2020, quando a Corte de Justiça da União Europeia invalidou o Privacy Shield, reiterando que nem a retórica de confiança mútua nem os interesses econômicos seriam suficientes para superar as incompatibilidades estruturais com os programas de vigilância estadunidenses (Greenleaf, 2021). Nesses episódios, percebe-se que a governança da privacidade não aparece como resultado de consensos automáticos, mas de disputas políticas em torno de qual regime prevalecerá na gestão da circulação global de dados.

Como vimos, essa fragmentação levou ao fortalecimento de mecanismos de certificação e auditoria como instrumentos de tradução normativa entre diferentes jurisdições. O ISO/IEC 27701[19], publicado em 2019, é exemplar nesse sentido, ao estender os requisitos

[19] Trata-se de uma norma internacional de extensão da ISO/IEC 27001 e ISO/IEC 27002, publicada em 2019, que estabelece requisitos e orientações para a gestão da privacidade da informação. Ela cria um Sistema de Gestão de Informações de Privacidade (PIMS – Privacy Information Management System), funcionando como um framework de governança da privacidade que pode ser integrado aos sistemas já existentes de gestão da

de segurança da informação da ISO 27001 para a proteção de dados pessoais, o padrão se converte em ferramenta global de demonstração de conformidade, utilizada por organizações que operam simultaneamente em diferentes marcos regulatórios (Bulow, 2021). Embora formalmente "voluntários", tais instrumentos tornam-se praticamente obrigatórios para o acesso a mercados internacionais, criando uma lógica de regulação por certificação. O APEC/CBPR (Cross-Border Privacy Rules)[20], por sua vez, aprofunda esse movimento ao estabelecer um sistema transnacional de reconhecimento mútuo, no qual autoridades nacionais designam organismos acreditadores e estes certificam empresas com base em um conjunto padronizado de requisitos (OECD, 2013). Como observa Büscher e Laidlaw (2020), a certificação não cria uma gramática de auditabilidade que legitima práticas ao torná-las "verificáveis" em vez de necessariamente justas ou proporcionais. A linguagem técnica da conformidade tende, assim, a ocupar o espaço da normatividade política, deslocando qualquer resquício de um debate político para o requisito técnico do cumprimento de um check list.

A demanda por adequação regulatória, por sua vez, implicou na expansão de um vasto mercado de serviços especializados - consultorias, escritórios de advocacia internacionais e, principalmente, as chamadas Big Four[21], que desenvolveram divisões inteiras dedicadas à proteção de dados e à gestão de risco informacional. Não por acaso, Greenleaf (2021) observa que, em diversos países do Sul Global, a aprovação de leis de privacidade foi acompanhada pelo crescimento imediato de cursos de certificação, treinamentos corporativos e manuais de adequação voltados a empresas multinacionais. Esse movimento reforça uma dependência estrutural na medida em que organizações locais tornam-se clientes de serviços de *compliance* que importam modelos e metodologias, frequentemente com pouca aderência às práticas sociais e econômicas locais, elevando o papel dos especialistas técnicos a um patamar central

segurança da informação, concebida para apoiar organizações na demonstração de conformidade com legislações como o GDPR europeu.

[20] Mecanismo internacional de governança da privacidade de dados desenvolvido no âmbito da APEC (Asia-Pacific Economic Cooperation), lançado em 2011. É um sistema voluntário que busca facilitar fluxos internacionais de dados pessoais entre as economias membros da APEC, conciliando a proteção da privacidade com a promoção do comércio digital. Funciona como uma espécie de selo de confiança, em que empresas podem se submeter a auditorias por entidades certificadoras reconhecidas ("Accountability Agents"), demonstrando que seguem os Princípios de Privacidade da APEC (semelhante ao GDPR europeu)

[21] Refere-se às quatro maiores empresas globais de auditoria, consultoria e serviços profissionais, com atuação decisiva em gestão de riscos, governança corporativa, tecnologia e conformidade regulatória. Incluem serviços de adaptação de empresas a normas de privacidade e proteção de dados, segurança da informação, anticorrupção e sustentabilidade, distribuídas em dezenas de países, atuando como atores privados transnacionais que moldam, de forma concreta, práticas de governança tanto em mercados locais quanto em regimes globais. Sikka (2009) e Power (1997) argumentam que esse papel das Big Four contribui para uma privatização da regulação, em que critérios técnicos e econômicos passam a substituir discussões públicas

na definição das fronteiras do aceitável. Como argumenta Mantelero (2020), o GDPR "*não apenas regula, mas cria mercados*", instaurando novas formas de dependência econômica em torno da expertise jurídica e tecnológica. O que se apresenta, portanto, como avanço normativo é também, simultaneamente, um processo de comodificação do cumprimento regulatório, no qual a proteção de dados se transforma em insumo para indústrias de auditoria e certificação.

A Global Privacy Assembly[22], que reúne autoridades nacionais de proteção de dados, é um exemplo de fórum informal que, apesar de não produzir normas vinculantes, difunde princípios e boas práticas que se tornam referências de fato para legisladores e reguladores (Raab, 2012). O mesmo ocorre no âmbito do Fórum de Governança da Internet (IGF), onde documentos orientadores e relatórios de melhores práticas circulam amplamente, moldando expectativas em âmbito transnacional (UNITED NATIONS, 2019), reforçando a perspectiva de uma infraestrutura normativa distribuída, na qual autoridades, especialistas, ONGs e empresas produzem e circulam conhecimento regulatório em um circuito global que, embora não coercitivo, exerce pressão significativa sobre Estados e organizações. Diante desse panorama, prosseguimos para o item 3.3 reside precisamente na constatação de que tais arranjos normativos não se limitam a fixar obrigações jurídicas ou institucionais. Eles configuram, antes, ecologias regulatórias que estruturam práticas organizacionais, distribuem capacidades entre atores e definem os termos em que a privacidade pode ser reivindicada. A multiplicidade de regimes, padrões técnicos e certificações compõem um campo no qual o discurso da proteção convive com a intensificação da circulação de dados, sempre em nome da confiança, da interoperabilidade e da previsibilidade regulatória. Essa é a base sobre a qual se pode, então, analisar como tais arranjos reverberam na constituição de formas de subjetivação e de responsabilização, articuladas no dispositivo privacidade que será explorado no item seguinte.

[22] A Global Privacy Assembly (GPA) é uma rede internacional que reúne autoridades de proteção de dados e privacidade de diversos países para debater, alinhar e promover princípios comuns de governança da privacidade em escala global. Ela existe desde 1979, quando foi criada como a International Conference of Data Protection and Privacy Commissioners (ICDPPC). Em 2019, passou a se chamar GPA, refletindo a ampliação de sua atuação para além da conferência anual — hoje a rede funciona de forma permanente, com grupos de trabalho temáticos, relatórios e resoluções, ajudando a legitimar certos padrões regulatórios — como a ênfase em accountability e em modelos de adequação —, ampliando o peso internacional de marcos como o GDPR europeu.

3.3 O caso do GDPR: introduzindo o dispositivo privacidade

Procuramos, até a presente seção, sugerir que os regimes internacionais de privacidade e proteção de dados não operam no vazio. Eles emergem no interior de uma economia política da informação em que a circulação de dados é infraestrutura de mercados e de políticas públicas (ver seção 2.2), e são objetos de disputa em arenas de governança atravessadas por assimetrias históricas e por diferentes projetos normativos (ver seção 2.3). A partir das duas seções preliminares deste capítulo, procuramos agora interpretar um dos principais instrumentos normativos de governança da privacidade e da proteção de dados à nível global como elementos articulados a um *dispositivo privacidade*, ou seja, um conjunto de técnicas, discursos e normas que convertem a extração de dados em governável, distribuindo responsabilidades e estabilizando expectativas de risco. Trata-se, em síntese, de um regime de veridicção e de normalização que configura a proteção de dados como condição operacional da sua captura. Couldry e Mejias resumem o conjunto de preocupações que norteiam a presente perspectiva:

> Embora ainda não esteja claro quão eficaz será o desafio imposto pelo GDPR às práticas de tratamento de dados do ponto de vista dos direitos humanos, como a privacidade, não há dúvida quanto à influência que sua publicação exerceu sobre o clima de um debate global em torno das questões de dados. Considere dois relatórios das Nações Unidas, de 2014 e 2018, ambos intitulados *"The Right to Privacy in the Digital Age"* (Alto Comissariado das Nações Unidas para os Direitos Humanos, 2014; 2018). O relatório de 2014 trata quase inteiramente da vigilância estatal; quando menciona as corporações (parágrafos 42 a 46), o foco está em saber se elas devem ou não atender aos pedidos governamentais de acesso a dados. (...) Em 2018, contudo, o enfoque se desloca, passando a incluir uma discussão sobre o crescimento das práticas corporativas de coleta de dados e sobre o seu correspondente "poder analítico". O relatório mais recente menciona "um crescente consenso global sobre padrões mínimos que devem reger o tratamento de dados pessoais por parte de Estados, empresas e outros atores privados" e insiste que a proteção de direitos humanos daí resultante "deve também se aplicar às informações derivadas, inferidas e previstas por meios automatizados, na medida em que tais informações se qualifiquem como dados pessoais" (parágrafo 30). Na prática, o relatório da ONU de 2018 encoraja os Estados a adotarem algo semelhante ao GDPR. Contudo, persistem lacunas importantes em suas recomendações: em nenhum momento o documento questiona a própria coleta de dados pelas empresas, nem reconhece como a coleta contínua de informações sobre e a partir das pessoas pode, por si só, comprometer valores como liberdade e autonomia — ainda que o texto cite o princípio fundamental do direito europeu segundo o qual "o indivíduo deve dispor de uma esfera de

> desenvolvimento, interação e liberdade autônoma" (COULDRY e MEJIAS, 2019, p. 6)

O GDPR europeu cristaliza, de maneira particularmente visível, a ambivalência central de nossa hipótese. Seu artigo 5(1) enuncia os princípios estruturantes do tratamento de dados: legalidade, lealdade e transparência, limitação de finalidade, minimização, exatidão, limitação da conservação e integridade, complementados pelo princípio de *accountability*, que obriga o controlador a demonstrar conformidade. Nele, temos que:

> Os dados pessoais devem ser:
> (a) processados de forma lícita, leal e transparente em relação ao titular dos dados ("licitude, lealdade e transparência");
> (b) coletados para finalidades específicas, explícitas e legítimas, e não tratados posteriormente de maneira incompatível com essas finalidades; o tratamento posterior para fins de arquivamento de interesse público, pesquisa científica ou histórica ou fins estatísticos não será considerado incompatível com as finalidades iniciais, de acordo com o artigo 89(1) ("limitação da finalidade");
> (c) adequados, pertinentes e limitados ao que for necessário em relação às finalidades para as quais são processados ("minimização dos dados");
> (d) exatos e, quando necessário, atualizados; devem ser tomadas todas as medidas razoáveis para garantir que os dados pessoais inexatos, tendo em vista as finalidades para as quais são tratados, sejam apagados ou retificados sem demora ("exatidão");
> (e) conservados em uma forma que permita a identificação dos titulares dos dados por não mais tempo do que o necessário para as finalidades para as quais os dados pessoais são tratados; os dados pessoais podem ser armazenados por períodos mais longos desde que sejam processados exclusivamente para fins de arquivamento de interesse público, pesquisa científica ou histórica ou fins estatísticos, em conformidade com o artigo 89(1), e mediante a implementação das medidas técnicas e organizacionais apropriadas exigidas por este Regulamento para salvaguardar os direitos e as liberdades do titular dos dados ("limitação da conservação");
> (f) processados de modo a garantir a segurança adequada dos dados pessoais, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidental, por meio da utilização de medidas técnicas ou organizacionais apropriadas ("integridade e confidencialidade"). (UNIÃO EUROPEIA, 2016. Tradução nossa.)

Essa formulação tem dupla função. Por um lado, oferece um repertório normativo de garantias que sustenta a reivindicação europeia de liderança no campo da proteção de dados, ao mesmo tem em que transforma a proteção de dados e da privacidade em gramática de gestão contínua de riscos e conformidades. A obrigação de "demonstrar conformidade" não se restringe a vedar práticas, mas exige a constituição de uma burocracia documental e

técnica voltada à previsibilidade da circulação informacional. Kuner (2017) e Lynskey (2015) apontam que essa ambivalência é estruturante, na medida em que o GDPR é frequentemente apresentado como a "Carta Magna" da proteção de dados, cuja lógica central corresponde a uma noção de *"compliance by design"*, segundo o qual direitos subjetivos estão condicionados à capacidade institucional de demonstrar conformidade. Farrell e Newman (2019), nessa mesma direção, evocam a ideia de *Brussels Effect*, destacando como a exportação desse modelo projeta, antes de qualquer coisa, regimes de padronização global.

Podemos, a partir dessa perspectiva, também recorrer, evidentemente, à leitura de Zuboff (2019), cuja formulação também traz insumos para interpretar que a regulação não interrompe a extração de dados, estabelecendo condições previsíveis para sua circulação continuada, constituindo uma instância de infraestrutura do poder regulatório (DeNardis, 2020), articulando a defesa de valores normativos em função da estabilização da economia digital global. Consolida-se uma ferramenta, nesse sentido, de governança neoliberal, na medida em que a "proteção" é convertida em técnica de gestão de risco, cálculo de proporcionalidade e avaliação contínua de impacto, respondendo de igual maneira às demandas de competitividade econômica e da circulação internacional de dados, consolidando a percepção da UE como mercado único digital, condicionante de relações comerciais transfronteiriças, organizando critérios de acesso (Lynskey, 2015), previsibilidade e interoperabilidade informacional (Kuber, 2017).

Essa lógica se evidencia ainda mais no artigo 6, que define as bases legais do tratamento. A presença do consentimento, da execução contratual e da obrigação legal sugere uma matriz de salvaguardas, no que se refere ao consentimento (art. 6(1)(a)), a execução contratual (art. 6(1)(b)), a obrigação legal (art. 6(1)(c)), o interesse vital (art. 6(1)(d)) e o exercício do interesse público (art. 6(1)(e)), condicionando o tratamento de dados a proporcionalidade da ação do Estado. Contudo, a inclusão do "interesse legítimo do controlador" (art. 6(1)(f)), detalhado no Recital 47, funciona como válvula de flexibilidade:

> Os interesses legítimos de um controlador, inclusive os de um controlador ao qual os dados pessoais possam ser comunicados, ou de um terceiro, podem constituir uma base jurídica para o tratamento, desde que não prevaleçam sobre os interesses ou os direitos e liberdades fundamentais do titular dos dados, levando-se em consideração as expectativas razoáveis dos titulares com base em sua relação com o controlador. Tal interesse legítimo pode existir, por exemplo, quando há uma relação relevante e apropriada entre o titular dos dados e o

> controlador — como nas situações em que o titular seja cliente ou empregado do controlador. De todo modo, a existência de um interesse legítimo deve ser cuidadosamente avaliada, incluindo-se a análise sobre se o titular dos dados pode razoavelmente esperar, no momento e no contexto da coleta dos dados pessoais, que o tratamento para essa finalidade venha a ocorrer. Os interesses e direitos fundamentais do titular dos dados podem, em particular, prevalecer sobre o interesse do controlador, especialmente quando os dados pessoais são tratados em circunstâncias nas quais os titulares não poderiam razoavelmente esperar um tratamento posterior. Considerando que cabe ao legislador estabelecer por lei a base jurídica para que as autoridades públicas tratem dados pessoais, essa base jurídica (do interesse legítimo) não deve ser aplicada ao tratamento realizado por autoridades públicas no desempenho de suas funções. O tratamento de dados pessoais estritamente necessário para fins de prevenção à fraude também constitui um interesse legítimo do controlador em questão. O tratamento de dados pessoais para fins de marketing direto pode ser considerado realizado com base em interesse legítimo. (UNIÃO EUROPEIA, 2016. Tradução nossa.)

O recital explicita, nesse sentido, que esse interesse pode incluir, por exemplo, situações em que exista "relação pertinente e apropriada" entre titular e responsável, bem como a "prevenção de fraude". Tal formulação transfere o equilíbrio da proteção para processos de avaliação contextual, dependentes da capacidade institucional das autoridades e do aparato probatório das organizações. O resultado é um modelo em que a expansão do tratamento se torna legítima sempre que for acompanhada de justificativas documentadas, avaliações de proporcionalidade e medidas mitigatórias. O dispositivo, portanto, mais uma vez reorganiza suas condições de aceitabilidade da captura. Kuner (2017) observa que o interesse legítimo é a mais controversa e flexível das bases legais do tratamento de dados, na medida em que confere aos controladores margem para justificar tratamentos de dados que vão além do consentimento explícito, desde que possam demonstrar equilíbrio "razoável "entre riscos e benefícios. Esse raciocínio desloca para o sujeito de dados a tarefa de ajustar suas expectativas ao contexto relacional em que se insere — como cliente, empregado ou usuário de serviço digital.

Em outras palavras, a subjetividade jurídica do indivíduo é moldada não como portadora de direitos absolutos, mas como parte de uma economia de expectativas administráveis. De Hert e Papakonstantinou (2012) argumentarão, em direção semelhante, que a cláusula do interesse legítimo converte direitos fundamentais em variáveis de cálculo, em que a legitimidade decorre da capacidade das organizações de demonstrar proporcionalidade e não da recusa categórica de certos tratamentos, reconfigurando a privacidade e a proteção como objeto de gestão contínua da violabilidade. A gramática da

proteção aparece subordinada a uma racionalidade da circulação e do risco e de expansão dos fluxos, a partir de garantias de *legitimação*. Ao lado da crítica de Passetti (2020) sobre uma ecopolítica do risco, pode-se sugerir que o Recital 47 materializa uma forma de subjetivação em que o indivíduo é chamado a ajustar suas expectativas e a aceitar como "pertinentes e apropriadas" práticas de coleta e análise de dados impostas por relações de consumo ou trabalho. O consentimento, como discutiremos, desloca responsabilidades para o sujeito; o interesse legítimo, por sua vez, condiciona o próprio campo do aceitável ao cálculo institucional, e o resultado é uma normatividade que contribui para a fabricação de sujeitos conformes à lógica da captura.

A centralidade atribuída ao consentimento como base legal paradigmática reforça essa perspectiva. Embora apresentado como salvaguarda da autonomia individual, o consentimento poderá operar, na prática, como mecanismo de transferência da responsabilidade regulatória para o sujeito de dado**s**, que deve compreender, avaliar e autorizar práticas frequentemente opacas e tecnicamente complexas. A figura do "titular" é, assim, a de um sujeito interpelado a gerir riscos pessoais, a navegar em interfaces de aceitação e a exercer escolhas que dificilmente são livres de assimetrias de poder ou de dependências cotidianas (MOROZOV, 2011). Interpretado nessa chave, o consentimento materializa um processo de subjetivação neoliberal, em que a liberdade jurídica formal corresponde à obrigação de autogoverno diante da difusão da vigilância. Emprestando, mais uma vez, de Passetti (2020), a subjetividade aparece como constituída no interior de arranjos normativos que moldam condutas e expectativas, convocando o sujeito a assumir a posição de gestor de sua própria exposição, responsabilizado por aceitar ou recusar termos efetivamente incontornáveis, num regime em que a proteção é recodificada como responsabilização individual permanente.

Essa figura do sujeito de dados como gestor de si é tensionada quando observamos o quanto as condições de consentimento são pré-formatadas por arquiteturas técnicas e jurídicas que não oferecem, de fato, alternativas substantivas (Cassino et al., 2021.) Como mostram análises críticas sobre o colonialismo de dados, o consentimento garante aparência de autonomia enquanto organiza mecanismos de exploração por meio de contratos de adesão, interfaces persuasivas e modulação algorítmica que induzem expectativas de aceitação, constituindo uma relação na qual a pretensão da liberdade coincide com a obrigação de administrar riscos e aceitar como "razoáveis" tratamentos de dados unilateralmente definidos

por empresas ou pelo Estado. O que temos, sugere Morozov (2011), Mejias e Couldry (2019) em síntese é uma economia política em que a responsabilização individual oculta cotidianamente assimetrias estruturais e transfere o peso da proteção da privacidade para escolhas quase sempre inevitáveis. Esse arranjo evidencia, como sugere Morozov (2011), que a retórica da liberdade digital frequentemente convive com práticas de controle e vigilância invisíveis, produzindo uma situação em que o discurso de direitos legitima infraestruturas que ampliam o poder das Plataformas. A ênfase no consentimento, nesse sentido, opera como tradução jurídica desse cenário, exigindo as condições de um autogoverno constante frente a estruturas que escapam ao controle do sujeito dos dados. Uma governamentalidade neoliberal-digital (Kosteczka, 2024), portanto, não diz respeito unicamente a organizar e legitimar fluxos de dados em conformidade às necessidades do extrativismo das plataformas, mas talvez principalmente a produzir subjetividades adequadas a consumidores que aceitam práticas de monitoramento como condição de sociabilidade, emprego, acessibilidade ou de cidadãos que se ajustam à vigilância em nome da segurança (Morozov, 2011).

Ao mesmo tempo, a ênfase em *accountability*, reforçada pelos artigos 24 e 25 do GDPR, aprofunda essa inflexão. Exige-se que controladores implementem "medidas técnicas e organizacionais apropriadas" (UNIÃO EUROPEIA, 2016) e que incorporem a proteção "desde a concepção e por padrão" (*privacy by design e by default*). Isso implica na criação de relatórios de impacto, registros de operações e processos de auditoria capazes de demonstrar diligência contínua. Correndo o risco da repetição excessiva, mais uma vez o GDPR atua, portanto, como dispositivo que internaliza a racionalidade do risco. A proteção da privacidade se converte em campo de *expertise* e mercado de consultorias que reconfiguram a própria infraestrutura de governança da internet. Mesmo a prerrogativa da proteção desde a concepção pode, dessa perspectiva, ser interpretada em termos de seus elementos de tecnologia de governo do risco, neste caso inclusive incorporada ao próprio ciclo de vida do dado, exigindo - conforme o art. 25 do GDPR, "medidas técnicas e organizacionais apropriadas" e regimes de registro e rastreabilidade que mantenham *logs* de coleta, consulta, alteração, divulgação e eliminação, de modo a estabelecer "justificativa, data e hora" de cada operação, identificar quem acessou e a quem se divulgou — e de igual maneira disponibilizar essa trilha à autoridade quando requisitada (em função de demandas de verificação de licitude, *self-monitoring*, integridade e até persecução penal).

O *privacy by design*, no artigo 25 do GDPR, projeta a proteção de dados como princípio estruturante da própria organização tecnológica e institucional do tratamento. O dispositivo estabelece que

> "taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation" (UNIÃO EUROPEIA, 2016, art. 25(1))

A formulação é exemplar da lógica de gestão de risco, ao exigir do controlador a incorporação de "medidas técnicas e organizacionais apropriadas" em função de variáveis de contexto, custo e viabilidade, evidenciando que a efetividade da proteção está vinculada a critérios de proporcionalidade, e não a interdições absolutas. O texto explicita ainda que tais medidas devem concretizar "*data protection principles, such as data minimisation*" (UNIÃO EUROPEIA, 2016, art. 25(1)) e integrar "*the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*" (ibid.). A proteção é, assim, descrita em termos de tarefa de cálculo institucional contínuo, em que a obrigação consiste em demonstrar sua adequação frente ao risco. A segunda dimensão normativa do artigo reforça essa inflexão, ao afirmar que*"o controlador deverá implementar medidas técnicas e organizacionais apropriadas para garantir que, por padrão, apenas os dados pessoais que sejam necessários para cada finalidade específica do tratamento sejam processados."* (UNIÃO EUROPEIA, 2016, art. 25(2)).

O princípio de *privacy by default*, portanto, condiciona não apenas a coleta, mas também a extensão, a duração e a acessibilidade do tratamento, impondo que "*by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*" (ibid.). Em termos de nossa hipótese, esse arranjo normativo organiza a aceitabilidade do fluxo de dados pela padronização ao formalizar uma arquitetura que permite circulação, legitimada pelo acompanhamento de registros, justificativas e barreiras procedimentais. O próprio regulamento prevê que "*an approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance*" (ibid.), reforçando que a conformidade deve ser comprovada por meio de certificações. Essa linguagem ecoa diretamente os *standards* produzidos em ambientes de padronização técnica,

como a série ISO/IEC 27000, dedicada à segurança da informação, ou as diretrizes da OCDE sobre governança de dados, em que a privacidade se traduz em *benchmarks* de eficiência e em métricas auditáveis, tornando direitos exequíveis não tanto por sua substância, mas por sua rastreabilidade documental, reiterando um movimento de "economização" da proteção de dados, internalizado pelas próprias organizações e verificado por terceiros acreditados, emissores de certificações técnicas, transformando mais uma vez a percepção do risco em oportunidade de produção de valor, reforçando o lugar da privacidade como "problema de gestão" e não como limite político ao extrativismo de dados.

Essa proximidade entre normas jurídicas e regimes técnicos de padronização permite compreender o GDPR como parte de um ecossistema normativo global que reforça racionalidades de circulação, interoperabilidade e competitividade. Assim como as normas ISO ou os guidelines da OECD, o regulamento europeu define a proteção em termos de "boas práticas" verificáveis, integradas a circuitos de comércio internacional e a mecanismos de reconhecimento extraterritorial (como o regime de adequação ou as cláusulas contratuais padrão). A questão das transferências internacionais, por sua vez, ilustra de forma particularmente clara como a lógica do *dispositivo privacidade* se estrutura em torno da administração de crises e da preservação da circulação.

A decisão Schrems II do Tribunal de Justiça da União Europeia, em julho de 2020, invalidou o Privacy Shield que desde 2016 regulava fluxos entre UE e EUA, declarando-o incompatível com os artigos 7 e 8 da Carta dos Direitos Fundamentais da União Europeia. O tribunal considerou que os programas de vigilância norte-americanos não ofereciam salvaguardas proporcionais nem meios efetivos de recurso para titulares europeus. A resposta institucional imediata foi a de reconfiguração dos fluxos, preservando as Cláusulas Contratuais-Padrão (SCCs), previstas no artigo 46(2)(c) do GDPR, agora condicionadas a avaliações de impacto específicas (*transfer impact assessments*) e à adoção de "medidas suplementares" de segurança, conforme detalhado nas Recomendações 01/2020 do Comitê Europeu de Proteção de Dados (EDPB). Esse arranjo deslocou a efetividade da norma para a documentação e para a capacidade das empresas de justificar, perante autoridades nacionais, que os riscos de acesso governamental extraterritorial estavam mitigados por criptografia forte, segmentação de dados ou mecanismos contratuais adicionais.

Em 2023, ainda, a Comissão Europeia aprovou a decisão de adequação para o EU-U.S. Data Privacy Framework (DPF), amparada no artigo 45 do GDPR. O DPF introduziu promessas de salvaguardas reforçadas, incluindo a criação de um *Data Protection Review Court* nos EUA, com competência para analisar reclamações de sujeitos de dados europeus e impor medidas corretivas vinculantes. Ainda assim, como observaram organizações da sociedade civil, persistem dúvidas sobre a suficiência dessas respostas diante da amplitude legal da vigilância norte-americana. A sequência destes dois episódios, em certo sentido, contribui para evidenciar a maneira pela qual crises jurídico-políticas no interior deste debate desencadearam recalibragem procedimentais que implicaram em novas camadas de documentação, auditoria e supervisão - ou seja, em camadas sucessivas de racionalização procedimental, mantendo o objetivo central de compatibilizar a economia digital transnacionais com uma retórica da privacidade e da proteção de dados como direitos fundamentais.

Essa mesma racionalidade aparece, em outro registro, na Convenção 108+. Entre suas "inovações" estão a inclusão explícita de "categorias especiais de dados" (como saúde, orientação sexual, opiniões políticas), a regulação das "decisões baseadas unicamente em tratamento automatizado", o fortalecimento da obrigação de notificação de violações e a previsão de "autoridades independentes e dotadas de recursos adequados" como condição mínima de efetividade. A Convenção 108+ também reforça princípios centrais já mencionados no GDPR — como limitação de finalidade, proporcionalidade e salvaguardas de segurança —, mas com a vocação de oferecer um núcleo constitucional comum que ultrapassa as fronteiras da União Europeia, sendo sua adesão aberta a países não europeus, projetando um horizonte de convergência global, ainda que marcado por assimetrias de implementação. A leitura conjunta dessas trajetórias pode sugerir que um *dispositivo privacidade* parece operar como tecnologia normativa de longo prazo, respondendo a crises de estabilidade e a novas instâncias e prerrogativas que reforçam a gramática da governança do risco. A Convenção 108+ desempenha, nesse contexto, o papel de uma infraestrutura de convergência mínima, enquanto o GDPR fornece o modelo de densidade normativa e o DPF exemplifica as negociações pragmáticas que preservam a circulação dos fluxos, evidenciando que a proteção de dados segue, a despeito de processos de adaptação, como condição de governabilidade da circulação.

Tomadas em conjunto, essas arquiteturas nos permitem caracterizar o *"dispositivo privacidade"* como tecnologia de administração do risco informacional em escala global, apesar de suas especificidades locais, (re)produzindo direitos e deveres (visibilidade, correção de assimetrias, salvaguardas técnicas), e parametrizando a circulação por bases legais elásticas, contratos padrão, certificações, mecanismos de adequação e autoridades de supervisão. Essa ambivalência se torna inteligível quando relembramos, dos itens 2.2 e 3.1, de uma racionalidade neoliberal que individualiza escolhas, monetiza a conformidade e transforma proteção em governabilidade de mercado, em função dos cenários que desenhamos na seção 2.3, em torno das assimetrias na gestão de quem define os padrões, quem os audita e quem arca com o custo do risco.

Nossa leitura não implica relativizar a existência dos direitos, mas evidencia que sua dimensão performática depende de condições de verificabilidade e de institucionalização. Essa formulação pode ser lida, como sugere Passetti et al (2020), na chave de uma governança contemporânea que fabrica dispositivos de rastreabilidade que produzem tanto segurança quanto sujeição. Ou seja, os direitos só adquirem concretude quando inscritos em arranjos de rastreamento contínuo, de tal modo que a proteção se confunde com o monitoramento administrado. Nesse mesmo registro, Stiegler (2018) enfatiza que o neoliberalismo reinscreve direitos sob o marco da adaptabilidade, convertendo-os em operadores de flexibilidade institucional. No campo da proteção da privacidade, portanto, à luz do discutido até o momento, sinaliza para um conjunto de garantias que depende de infraestrutura documental e de regimes de verificação que deslocam a autonomia para a capacidade de alinhar-se a padrões. Assim, direitos de acesso, retificação ou oposição tornam-se eficientes apenas quando inseridos em um ecossistema de validação que é, em si, parte da racionalidade neoliberal de governo. Aplicado ao campo da privacidade, esse diagnóstico mostra que a auditabilidade e a explicabilidade podem funcionar mais como garantias para instituições do que como quaisquer garantias para os sujeitos dos dados (Morozov, 2011).

A análise desenvolvida até aqui procurou mostrar que a privacidade e a proteção de dados vem operando como vetor de subjetivação e responsabilização, articulando práticas de autogoverno coerentes com a racionalidade neoliberal. Nesse registro, a ênfase em consentimento, accountability e gestão de riscos desloca a proteção de dados do campo dos direitos inalienáveis para a esfera da performance, exigindo sujeitos permanentemente

responsivos às demandas normativas e técnicas. Como argumentamos, esse deslocamento não consolida a lógica de governamentalidade em que o indivíduo é interpelado como administrador de sua própria exposição à incerteza. Ao compreender a privacidade como dispositivo, evidenciamos o caráter ambivalente de sua função contemporânea: simultaneamente promessa de proteção e mecanismo de intensificação do controle. Essa reflexão prepara o terreno para nosso breve mergulho sobre a experiência brasileira, no interior da qual o *dispositivo privacidade* se enraíza em trajetórias institucionais marcadas por heranças autoritárias, digitalização acelerada da esfera pública e disputas normativas recentes. O Capítulo 4 examinará como, no Brasil, a inscrição da privacidade em marcos legais e estratégicos – do Marco Civil da Internet à Lei Geral de Proteção de Dados (LGPD), entre outros – não pode ser dissociada das continuidades securitárias da virada para a redemocratização, nem das condições globais de colonialismo de dados. Trata-se, portanto, de um arranjo tecnopolítico específico, no qual a privacidade é mobilizada como recurso estratégico, ora para legitimar práticas de vigilância e controle, ora para responder a pressões sociais e internacionais. É no cruzamento, portanto, entre subjetivação neoliberal e governamentalidade digital-securitária que situamos a experiência brasileira, como inflexão precisa para ilustração da presente tese.

4. A experiência brasileira da governança de dados: disputas, normativas e governamentalidade

Nos capítulos anteriores buscamos reconstruir, de certa forma, os deslocamentos da segurança como tecnologia de governo e a formação de um dispositivo global da privacidade, coerente com uma determinada formatação da governança da Internet. Aqui o objetivo é examinar brevemente como essas dinâmicas se materializam em um contexto específico, atravessado por disputas políticas internas, heranças autoritárias e pressões externas de regimes normativos internacionais.

Trata-se de compreender como a privacidade é posicionada, no Brasil, ora como vulnerabilidade estratégica a ser controlada, ora como promessa de direitos fundamentais a serem resguardados, resultando em arranjos instáveis e por vezes contraditórios. Serão analisados os arranjos tecnopolíticos contemporâneos da digitalização do Estado, que articulam inovação, eficiência e controle, mas frequentemente resultam na expansão de infraestruturas de vigilância sob a lógica securitária. Por fim, o foco recai sobre o paradigma da proteção de dados e da privacidade, representado sobretudo pela Lei Geral de Proteção de Dados (LGPD) e pela criação da Autoridade Nacional de Proteção de Dados (ANPD), cuja configuração revela a complexa negociação entre demandas da sociedade civil, interesses empresariais e estratégias governamentais de segurança.

Com isso, pretende-se demonstrar que a experiência brasileira não pode ser compreendida apenas como um reflexo tardio de marcos internacionais, mas como um campo de disputas em que se entrelaçam múltiplos vetores. A partir dessa perspectiva, o capítulo analisa a forma como dispositivos normativos são concebidos, apropriados e tensionados na experiência brasileira, revelando sua dimensão de alinhamento com a perspectiva da governamentalidade neoliberal.

4.1 Antecedentes institucionais e heranças autoritárias

É no interior de uma experiência não democrática, no Brasil, que se dão os primeiros passos da discussão sobre a gestão de dados pessoais, sobretudo marcada pelo contexto político e institucional típico da Doutrina de Segurança Nacional (Zanatta, 2022; Doneda, 2021). Ainda que não nos caiba, aqui, uma recuperação exaustiva do referido contexto, para fins da presente reflexão basta considerarmos que o cenário de escalada autoritária

(Skidmore, 1988) encontrou no uso de informações para fins políticos uma prática privilegiada, centralizado no Serviço Nacional de Informação (SNI), órgão da presidência da República, criado em 1964, sob o General Golbery Couto e Silva. Zanatta resume,

> Em uma lógica praticamente cibernética - de *feedbacks* e reavaliação permanente -, ele pretendia registrar e analisar informações de modo a dar uma estimativa da situação nacional. Chamado de Ministério do Silêncio, o SNI foi criado a partir de ampla dotação orçamentária e de um corpo de especialistas que produzia relatórios que formavam, nas palavras do historiador Carlos Fico, uma rede intertextual produtora de eficazes efeitos de sentido e de convicção (ZANATTA, 2022, p. 45)

Ao mesmo tempo, o DOI-Codi implicou em uma reconstrução assertiva do fluxo de informações no interior do Estado, instrumental para o aparato repressivo e de tortura, alimentado por fichas de dados pessoais (Godoy, 2014). No interior deste processo, os primeiros esforços de governança e proteção de dados pessoais no país respondem ao debate sobre a unificação das bases de registros civis, na forma do Registro Nacional de Pessoas Naturais (Renape) (Vianna, 2016), *"anunciado em um momento político de alta tensão, com o crescimento do MDB e (...) o fechamento do Congresso, em abril de 1977, com base no Ato Institucional n.5"* (Zanatta, 2022, p. 48). O Renape era interpretado como um sistema inovador, sob um Serviço Federal de Processamento de Dados (Serpro) profundamente comprometido, à época, com a automação de serviços federais e a ampliação da instrumentalização de dados no setor público (Vianna, 2016; Zanatta, 2022.). Evidencia-se, entretanto, a insuficiência de informações a disposição do público sobre o projeto, incorrendo na percepção crescente dos riscos implicados:

> Por trás do discurso asséptico e tecnocrata dos militares - de uma arquitetura de sistemas capaz de garantir efetividade às políticas públicas e atingir os anseios do bem comum - havia um histórico autoritário de vigilância, perseguição de lideranças e ruptura com o pouco que restava das instituições democráticas (ZANATTA, 2022, p. 49)

No final da década de 1970, portanto, em meio ao endurecimento da vigilância estatal, a oposição ao uso concentrado da informação emergiu justamente entre técnicos e engenheiros envolvidos na implantação dos sistemas de processamento de dados. Ao contrário do que se poderia supor, não foram apenas intelectuais externos ao aparato burocrático que perceberam os riscos da centralização. Profissionais do Serpro e de outros centros de informática governamental, além de articulistas de publicações técnicas começaram a chamar atenção para a possibilidade de que a informatização (Vianna, 2016; Zanatta, 2022), em vez de

representar progresso administrativo, se transformasse em uma engrenagem de vigilância permanente (Ripper, 2020; Oliveira, 2020). A experiência prática desses funcionários os colocava em posição privilegiada para identificar as consequências da concentração de informações sensíveis em grandes bancos de dados. Ao observarem o projeto do Renape, por exemplo, perceberam que a integração indiscriminada de informações fiscais, previdenciárias e eleitorais poderia dar origem a um mecanismo de monitoramento onipresente. O receio não era abstrato: tratava-se de avaliar, a partir do contato cotidiano com os sistemas, o potencial de cruzamento e monitoramento que o Estado passava a concentrar (Zanatta, 2022; Doneda, 2021). Mais do que qualquer coisa, o protagonismo técnico revelava que a discussão sobre privacidade e proteção de dados não poderia mais ser reduzida a um problema abstrato de garantias jurídicas, se configurando desde o início como um dilema tecnopolítico de primeira ordem.

O que emerge, portanto, é a constatação de que a resistência à centralização autoritária de dados nasceu também dentro da própria comunidade responsável por estruturar os sistemas. Esse dado histórico é relevante porque revela que, desde seu ponto de partida, a proteção de dados no Brasil foi percebida como um problema transversal, situado na intersecção entre técnica, política e direito. Esse entrelaçamento antecipou debates que décadas depois ganhariam centralidade com a LGPD, como veremos mais adiante. É, entretanto, nesse cenário de inquietação que surge o primeiro projeto legislativo brasileiro voltado especificamente para a proteção de dados pessoais: o Projeto de Lei nº 4.365/1977. A proposta não foi concebida em isolamento, tendo resultado de diálogos com a chamada comunidade de informática, que acompanhava com atenção as tendências internacionais e reconhecia a urgência de uma normatização preventiva. Inspirado por marcos como o *Privacy Act* norte-americano de 1974 e a lei francesa *Informatique et Libertés* de 1978, o PL representava uma tentativa de inserir o Brasil no debate emergente sobre limites democráticos à coleta e uso de dados (Zanatta, 2022, Doneda, 2021; Doneda, 2018). Nosso autor resume:

> (...) nota-se que a proposta se aproximava de uma espécie de junção de elementos de licenciamento e registro, ainda com uma forte crença na capacidade estatal de verificar as finalidades específicas dos bancos de dados. A regra básica era o licenciamento e o controle de finalidade. A proposta do deputado era criar um Registro Nacional de Banco de Dados para todos os órgãos governamentais, todas as sociedades de direito público, todas as "agências de detetives ou organizações encarregadas de realizar pesquisas sobre moralidade, recursos ou conduta de outrem" (...) O Registro deveria conter um conjunto de informações, como

> informações sobre o proprietário do banco de dados, pessoas responsáveis pela administração, local onde está situada a operação, características técnicas do banco de dados, reguladas posteriormente por resoluções, natureza do banco e finalidade do tratamento. (ZANATTA, 2022, p. 57.)

Estruturado em 17 artigos, o PL propunha um modelo regulatório baseado em licenciamento e controle de finalidade. Isso significava que determinados usos de dados pessoais deveriam ser previamente autorizados por uma autoridade pública, e que o tratamento de informações só poderia ocorrer dentro das finalidades declaradas e autorizadas. Esse desenho buscava impedir que a coleta de dados fosse desviada para propósitos não previstos ou abusivos, criando uma camada de proteção que combinava transparência e supervisão institucional (Vianna, 2016, Oliveira, 2020). Era, portanto, uma proposta avançada para o contexto brasileiro, que antecipava preocupações que só décadas mais tarde se consolidariam em normas internacionais, como a exigência de base legal e a limitação de finalidade. O PL 4.365/1977 também refletia a percepção de que a informatização não podia ser regulada apenas por normas de direito administrativo. A emergência de novas tecnologias exigia instrumentos jurídicos específicos, capazes de lidar com riscos inéditos, de modo que o projeto materializava o esforço de setores técnicos e políticos de criar uma moldura institucional para o uso da informação em larga escala, ainda que em um ambiente político marcado pelo autoritarismo (Doneda, 2021; Oliveira, 2020; Zanatta, 2022). A proposta, entretanto, carregava uma ambiguidade fundamental, dado eu era concebida dentro de um regime em que as liberdades civis não estavam em pauta, colidindo sua inspiração liberal-democrática com o ambiente político da Ditadura Militar.

Para tentar contornar as (incontornáveis) objeções, se colocou na mesa a possibilidade de uma Proposta de Emenda Constitucional (PEC) que desse sustentação ao novo modelo, criando bases constitucionais que permitissem o licenciamento de bancos de dados e a supervisão centralizada de sua utilização. No entanto, a proposta não avançou, e o projeto acabou sendo abandonado. A proposta demonstrava a capacidade de certos setores de antecipar riscos e de propor soluções inspiradas em modelos internacionais, mas também deixava claro que tais iniciativas não tinham condições políticas de prosperar. A ausência de abertura democrática inviabilizava a criação de instituições independentes capazes de exercer fiscalização. O destino do PL pode ser lido como sintoma da trajetória irregular que caracterizou a proteção de dados no Brasil (Zanatta, 2022; Doneda, 2016; Doneda, 2021):

marcada por momentos de avanço normativo, resistências políticas e pela prioridade atribuída à segurança do Estado.

O início da década de 1980 marca um período decisivo para compreender por que a proteção de dados pessoais não se afirmou como eixo estruturante da transição política brasileira. O movimento de abertura, conduzido sob a lógica da "lenta, gradual e segura" redemocratização, colocou na agenda nacional questões como a anistia, o enfrentamento das desigualdades sociais e a reorganização do sistema sindical. Nesse ambiente, a privacidade e o controle da informação eram reconhecidos como temas emergentes, mas não alcançaram prioridade suficiente para se converter em direitos institucionalizados. Como nota Zanatta (2022), entre 1980 e 1985 consolidou-se um quadro de limitações que explica a fragilidade das tentativas de afirmação desse campo: a inclusão formal e insuficiente de garantias na Política Nacional de Informática, a multiplicação de projetos de lei sem tramitação bem-sucedida e, diante do fracasso em nível federal, a busca por alternativas em estados e municípios. A chamada Política Nacional de Informática, sancionada em 1984, poderia ter sido o espaço privilegiado para consagrar mecanismos de proteção de dados, limitando-se entretanto a fórmulas genéricas que não ofereciam instrumentos concretos de garantias ou salvaguardas (Zanatta, 2022; Doneda, 2021; Saur, 1984). Como observa a literatura - majoritariamente do campo jurídico -, as normas resultantes se mostraram meramente declarativas e falharam em produzir uma infraestrutura regulatória efetiva. Nesse sentido, a política de informática opera em termos do símbolo da modernização tecnológica do país, mais do que efetivamente como garantia de direitos no ambiente digital.

4.2. A digitalização do Estado brasileiro e algumas condições de possibilidade para uma Lei Geral de Proteção de Dados

O ano de 2013 se tornou, por razões distintas e simultâneas, um marco de reconfiguração da agenda normativa em torno da governança dos dados no Brasil. No plano doméstico, as jornadas de junho (protestos em dezenas de cidades) foram recebidas com respostas coordenadas de segurança, multiplicando práticas de observação e mapeamento de manifestações; no plano internacional, as revelações de Edward Snowden sobre a NSA exibiram a vulnerabilidade do Brasil a coletas extraterritoriais, inclusive sobre autoridades de Estado e empresas estratégicas (como a Petrobras). A repercussão política foi imediata na forma do cancelamento de visita de Estado a Washington, CPI da Espionagem no Congresso

e uma agenda diplomática que resultou na liderança — ao lado da Alemanha — da resolução 68/167 da Assembleia Geral da ONU em 2013, pautando a agenda sobre privacidade na era digital dali em diante.

O período de 2013 a 2020 assistiu também à reengenharia administrativa do Estado federal no trato de dados pessoais e bases cadastrais, estruturando-se em arranjos tecnopolíticos que em geral articularam inovação, eficiência e controle, a partir de conjuntos de normativas e documentos orientadores de boas práticas que enfatizam a modernização administrativa e a oferta de serviços digitais como caminhos para aumentar produtividade econômica, inclusão e eficiência do setor público. Por exemplo, a *Estratégia Brasileira para a Transformação Digital (E-Digital)* de 2018 destaca que *"as tecnologias digitais proporcionam as ferramentas para uma profunda transformação na atuação do próprio governo, na competitividade e produtividade das empresas"*, visando que todos *"possam se desenvolver e prosperar"*. Dessa perspectiva, a privacidade e a proteção de dados aparecem instrumentalizadas como pré-requisitos para segurança no ambiente digital, condição vista como indispensável, sobretudo, para viabilizar serviços públicos digitais e dinamizar a inserção nacional na economia informacional.

Essa convergência entre eficiência administrativa e segurança informacional se reflete, de igual maneira, em outros marcos normativos da experiência brasileira. O Marco Civil da Internet (Lei 12.965/2014), por um lado, consagrou uma narrativa de direitos fundamentais dos cidadãos-sujeitos-usuários – como a proteção da privacidade e dos dados pessoais – e reconheceu a *"escala mundial da rede"* e os padrões internacionais como elementos estruturantes da governança da internet. Por outro lado, o mesmo instrumento incorporou dispositivos de monitoramento impondo deveres de guarda de registros, retenção de logs de conexão por um ano e provedores de aplicações por seis meses. Esses requisitos de retenção de dados, regulamentados posteriormente pelo Decreto 8.771/2016, sugerem mais uma vez a justaposição de uma governança de salvaguardas com uma governança de riscos no ambiente digital. Em nome da segurança e da investigação, foram expandidas técnicas de verificação e rastreabilidade dos usuários, ao mesmo tempo em que se afirmavam princípios de neutralidade e privacidade. A literatura (MAIA et al., 2016; Silveira, 2014) identifica nesse arranjo a possibilidade de uma convergência estrutural – e não mera contradição episódica – entre a tutela de direitos e a intensificação de práticas de monitoramento.

O esforço em nome da eficiência impulsionou, ao mesmo tempo, políticas de integração massiva de dados pessoais, frequentemente justificadas pelo discurso da inovação. Um exemplo paradigmático é o do Decreto 10.046/2019, que instituiu o Cadastro Base do Cidadão, visando à *"interoperabilidade"* de cadastros de bases públicas e à formação de um cadastro único nacional vinculado ao CPF, sob o argumento de evitar redundâncias e aprimorar o exercício das políticas públicas, propondo consolidar uma infraestrutura de dados abrangente. Na prática, o Cadastro Base do Cidadão funciona como uma infraestrutura de dados abrangente que integra múltiplas fontes de informação. Inicialmente, a base seria alimentada pelos dados biográficos vinculados ao CPF (como nome, nascimento, filiação, etc.), mas a previsão é de expandir esse repositório com informações de outras bases temáticas do governo (Internetlab, 2024) Em outras palavras, trata-se de uma base integradora e uma plataforma de interoperabilidade que permite o intercâmbio de dados entre diversos bancos de dados governamentais antes isolados (Internetlab, 2024; Data Privacy, 2023) Dessa forma, o Decreto 10.046/2019 contribui com a consolidação em nível federal um grande cadastro unificado de cidadãos, que reúne ampla variedade de dados pessoais em nome da eficiência administrativa.

Esse arranjo reforça elementos de uma racionalidade que prioriza a eficiência, inovação de mercado e participação do setor privado, enquanto parte da responsabilidade pela gestão de riscos é transferida a indivíduos e organizações. A Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637/2018, também explicita o referido processo. Em seus elementos centrais, a PNSI alinha a soberania nacional e o respeito aos direitos fundamentais – incluindo liberdade de expressão, proteção de dados pessoais, privacidade e acesso à informação – com diretrizes de segurança de Estado, como a cooperação entre órgãos de investigação e a orientação gerencial na proteção da informação. De um lado, reconhecem-se valores democráticos como a inviolabilidade da vida privada, da honra e da imagem; de outro, o decreto introduz o conceito de *"need to know"* para acesso a informações sigilosas e enfatiza a integração das inteligências (isto é, a cooperação entre os órgãos de segurança), preparando terreno para eventuais exceções a direitos em nome da segurança do Estado.

O Programa de Privacidade e Segurança da Informação (PPSI), por sua vez, lançado em 2023 (Portaria SGD/MGI nº 852/2023), aprofunda essa dinâmica de governamentalidade distribuída. O PPSI estabelece um arcabouço de controles e um ciclo contínuo de melhoria,

baseado em autoavaliação, análise de lacunas, planejamento e implementação de medidas de privacidade e segurança. Em outras palavras, cada órgão público deve diagnosticar seu próprio nível de conformidade e aprimorá-lo constantemente, elevando seu grau de maturidade nesses temas. De fato, as etapas internas do programa seguem a lógica PDCA (Planejar - Fazer - Checar - Agir) de aperfeiçoamento contínuo, de modo que as instituições permaneçam *"sempre em evolução usando o aprendizado de ações anteriores"*. Os valores anunciados pelo programa – *maturidade, resiliência, efetividade, colaboração e inteligência* – reforçam a ideia de uma gestão *tecnocrática* da privacidade, pautada em métricas de desempenho e adoção de boas práticas, considerando a proteção de dados um tema de gestão interna, integrando-a à cultura institucional de resultados e riscos.

Nesse sentido, o PPSI do governo federal enfatiza a difusão de guias, modelos e treinamentos, buscando criar uma verdadeira *"cultura de privacidade e segurança"* entre os servidores públicos. Entre as linhas de ação do programa estão a elaboração de normas e políticas internas, o desenvolvimento de metodologias (guias e modelos nacionais), mecanismos de maturidade (autoavaliações e planos de ação), investimentos em tecnologia (detecção e resposta a incidentes) e foco em pessoas (capacitação e retenção de talentos em privacidade e segurança). A ideia central é responsabilizar os indivíduos para que ajam proativamente na proteção de dados, adotando comportamentos seguros e seguindo protocolos estabelecidos. Esse processo contínuo de conscientização e capacitação visa, em última instância, que cada pessoa seja guardiã de si mesma e das informações sob seu cuidado. Como afirma o guia de boas práticas do programa, *"agir de forma proativa e preventiva, antevendo problemas, evita transtornos, auditoria externa e multas"* (BRASIL, 2023) – em um claro apelo à autorregulação. A metáfora de auditoria externa como "transtorno" reforça a noção de que a conformidade voluntária e antecipatória é a via ideal de adequação a norma.

No contexto do PPSI, a privacidade é, então, em grande medida, convertida em sinônimo de conformidade regulatória e gestão de risco, inserida em parâmetros globais de governança de dados. A Diretoria de Privacidade e Segurança da Informação (DEPSI) do governo federal, nessa direção, afirma a pertinência de adequação às *"melhores práticas internacionais em matéria de privacidade, segurança da informação e proteção de dados"*, incorporando-as em seus guias e modelos nacionais. Essas referências incluem desde padrões técnicos como normas ISO/IEC, normativas do National institute of Standards and

Technology (EUA) e os 18 controles de segurança do CIS (Center for Internet Security)[23], e diretrizes de organismos multilaterais, como as recomendações da OCDE sobre privacidade e as orientações do Comitê Europeu. O próprio governo reconhece que tais medidas decorrem da experiência prática global e de um *"amplo debate entre organismos e fóruns internacionais, governos, entidades especializadas, empresas e profissionais técnicos"*. Em outras palavras, a política doméstica de privacidade, em certo sentido, parece pautar-se por um consenso transnacional sobre o que seria a "boa" governança de dados, como discutida na seção 2.3.

Essa transnacionalização das referências, como vimos, não é necessariamente um sintoma de práticas de boa vizinhança. Ela evidencia a circulação de modelos normativos e a influência de interesses econômicos globais na definição do que se considera proteção de dados adequada – frequentemente alinhada a padrões hegemônicos. Fóruns internacionais como a Global Privacy Assembly (que reúne autoridades nacionais de proteção de dados) e o Fórum de Governança da Internet (IGF), embora não produzam normas vinculantes, atuam na harmonização de expectativas, por exemplo, ao difundir *"princípios e boas práticas que se tornam referências de fato para legisladores e reguladores"*, ou *"reforçando a perspectiva de uma infraestrutura normativa distribuída, na qual autoridades, especialistas, ONGs e empresas produzem e circulam conhecimento regulatório ... [que] exerce pressão significativa sobre Estados e organizações"* (Global Privacy Assembly, 2019). O resultado desse processo global é a formação de uma infraestrutura normativa distribuída de escala planetária, em que múltiplos atores – governos, empresas, comunidades epistêmicas e organizações da sociedade civil – modulam os padrões e expectativas em torno da privacidade. Nesse sentido, o discurso da privacidade e da proteção de dados convive com a intensificação da circulação de informações, sempre em nome de valores como confiança, interoperabilidade e previsibilidade regulatória. Em suma, vemos no caso brasileiro a repetição da tendência da privacidade como elemento de uma governança global de risco, na qual a conformidade normativa e a gestão técnica são condições para a própria circulação e uso dos dados no mercado global contemporâneo.

[23] são um conjunto de práticas recomendadas para fortalecer a cibersegurança de organizações — sejam instituições estatais, empresas ou outros agentes que manejam dados e sistemas. Eles foram desenvolvidos pelo Center for Internet Security (CIS), uma entidade sem fins lucrativos voltada a promover boas práticas de segurança na infraestrutura de TI

Este percurso revela como o discurso da privacidade foi progressivamente assimilado ao projeto de modernização gerencial do Estado, transformando-se em um instrumento de legitimação de práticas de eficiência, inovação e *accountability*. A governança dos dados pessoais passa a ser concebida como dimensão técnica da administração pública, orientada por métricas de desempenho, planos de conformidade e ciclos contínuos de melhoria. Essa transição traduz a ascensão de uma racionalidade regulatória de tipo neoliberal, em que a proteção da informação é tratada como ativo de confiança institucional e a aderência a padrões internacionais se torna indicador de maturidade administrativa. A LGPD, nesse contexto, emerge como síntese e catalisador desse processo, consolidando uma cultura de *compliance* informacional, elevando a gestão de riscos ao principal modo de governo dos dados. É nesse horizonte que o capítulo seguinte examina a LGPD não apenas como marco jurídico, mas como expressão paradigmática da governamentalidade tecnocrática que redefine a relação entre o Estado brasileiro e a circulação de dados.

4.3 O caso da LGPD: instrumentos e implicações à luz do *dispositivo privacidade*

Buscamos, até aqui, situar a LGPD e a ANPD em seu terreno histórico, em um contexto em que emerge um paradigma de governo por dados que aciona, sem grandes fricções, narrativas de direito e de risco. Autores que participaram da formulação de políticas digitais já alertavam para o desequilíbrio estrutural entre titulares e tratadores, enfatizando que a proteção efetiva exige governança de ciclo de vida (coleta, minimização, finalidade, segurança, descarte) e controles institucionais independentes (Doneda, 2006; Bioni, 2021; Rená, 2014). Quando esse ecossistema institucional se organiza ao mesmo tempo pela integração massiva de cadastros (Decreto 10.046/2019), pela retórica de interoperabilidade e por centros de comando que operam como interfaces de intermediação informacional, a fronteira entre exceção e rotina torna-se possivelmente instável. Nesse cenário, rupturas autoritárias não dependem de rupturas explícitas, podendo se manifestar como modulações administrativas que ampliam o acesso, alongam a guarda, flexibilizam a finalidade e naturalizam a vigilância *como requisito técnico de gestão.*

A centralização de cadastros, a criação de plataformas e a difusão de dispositivos de vigilância em megaeventos e emergências sanitárias revelam a transição de para uma lógica de governança por dados, na qual eficiência e proteção são mobilizadas como justificativas de

legitimação, ainda que ampliem as condições de coleta e rastreamento. Quando observada a partir de uma chave crítica, a digitalização das estruturas do estado se revela como um campo de arranjos tecnopolíticos, nos quais práticas de governo, racionalidades neoliberais e dispositivos de vigilância se entrelaçam na produção de novas formas de gestão populacional. A digitalização constitui, em síntese, a possível atualização das técnicas de poder, permitindo que procedimentos de catalogação, classificação e monitoramento — que já tinham lugar em regimes autoritários — sejam reconfigurados em ambientes de interoperabilidade de dados, plataformas digitais e sistemas algorítmicos. O desenvolvimento de plataformas estatais unificadas, que progressivamente se consolidam como principal interface entre cidadãos e serviços públicos, exemplifica esse processo (Bioni, 2021 Zanatta, 2022). A centralização de identificadores e a convergência de bases, entretanto, contribuem com a produção de condições para o exercício ampliado de vigilância administrativa, ainda que formalmente enquadradas na linguagem da modernização. Essa racionalidade se expressa na exaltação da integração de registros como forma de "reduzir custos" e "eliminar redundâncias", mas que silenciam sobre os riscos de concentração informacional e sobre a ausência de salvaguardas robustas contra usos abusivos. Como registram relatórios do InternetLab (2017) e do Data Privacy Brasil (2021), a integração informacional avança mais rápido que os mecanismos de accountability, resultando em um regime de vigilância em que as responsabilidades são, sobretudo, difusas. A criação da Lei Geral de Proteção de Dados (LGPD) e da Autoridade Nacional de Proteção de Dados (ANPD), entre 2018 e 2020, pode ser lida no interior desse pano de fundo. Ao mesmo tempo em que é interpretada como uma conquista normativa relevante, alinhada a tendências globais de proteção de dados, a LGPD também expressa a incorporação de padrões regulatórios que estabilizam a legitimidade da extração de dados, mas não rompem com assimetrias estruturais (Couldry e Mejias, 2019).

Retornando efetivamente ao percurso que culmina na criação da Lei Geral de Proteção de Dados (LGPD) e da Autoridade Nacional de Proteção de Dados (ANPD), ressalta-se que não se trata de um processo linear, mas atravessa diferentes regimes normativos e conjunturas políticas. Com a Constituição Federal de 1988, a literatura identifica uma inflexão normativa fundamental (Bioni, 2021). Os dispositivos constitucionais que tratam da privacidade (art. 5º, X), do sigilo das comunicações (art. 5º, XII) e do *habeas data* (art. 5º, LXXII) representaram a tentativa de romper com o legado autoritário da vigilância, ao inscrever a proteção de dados em um patamar de direito fundamental. O *habeas data*, em especial, introduziu um

mecanismo inovador de controle sobre informações pessoais, ao permitir acesso e retificação em registros públicos, antecipando discussões que se tornariam centrais, mais tarde, no texto da LGPD. Contudo, esse marco jurídico convivia com instituições ainda frágeis, pouco capazes de efetivar tais garantias de modo sistemático. Nos anos 1990, o Código de Defesa do Consumidor traz uma nova dimensão ao debate (Zanatta; 2022; Doneda, 2021; Bioni, 2021). Seu art. 43 disciplinou o direito de acesso e correção de informações em bancos de dados de consumo, introduzindo na prática a noção de que os indivíduos possuem titularidade sobre os dados que os identificam em relações contratuais. Embora circunscrito ao campo das relações de mercado, o instrumento reconhecia os riscos de assimetrias informacionais entre empresas e consumidores, estabelecendo direitos que antecederam a ideia de autodeterminação informativa.

A partir de 2004, a discussão sobre proteção de dados ganha fôlego regional, com as diretrizes do Mercosul que recomendaram padrões mínimos de salvaguardas e incentivaram a harmonização regulatória entre países do bloco. Esse movimento se inscrevia em um contexto de crescente influência europeia, marcado pela Diretiva 95/46/CE, e revelava a percepção de que a proteção de dados já se articulava a fluxos econômicos internacionais e à necessidade de adequação normativa para garantir integração comercial. No início da década de 2010, a promulgação da Lei de Acesso à Informação (Lei 12.527/2011, LAI) contribuiu para reforçar a ideia da transparência como um valor democrático, colocando em evidência as tensões entre a abertura de informações públicas e a proteção de dados pessoais. A partir desse momento, a governança informacional passou a ser disputada entre narrativas de publicidade e de privacidade, antecipando dilemas da compatibilização entre *accountability* e garantias individuais, que marcariam posteriormente a harmonização entre a LAI e a LGPD (Zanatta; 2022; Doneda, 2021; Bioni, 2021)

Dois anos depois, em 2014, o Marco Civil da Internet é frequentemente entendido como um divisor de águas. Reconhecido internacionalmente, o Marco Civil consolidou princípios de neutralidade de rede, privacidade e liberdade de expressão como direitos fundamentais no ambiente digital. Fortemente influenciado pelo contexto global das revelações de Edward Snowden sobre os programas de vigilância da NSA, que afetaram diretamente o Brasil, o Marco estabelecia fundamentos normativos que seriam posteriormente incorporados pela LGPD, ao estruturar direitos e deveres e ao afirmar a proporcionalidade como parâmetro para o tratamento de dados. A aprovação da LGPD, por sua vez, representa o

salto final para um regime geral de proteção de dados, impulsionada pelo escândalo da *Cambridge Analytica*, que expôs a nível internacional riscos associados ao uso abusivo de dados pessoais, e também pela pressão internacional por mecanismos de adequação, sob pena de isolamento do Brasil em fluxos globais de informação. Em 2022, a Emenda Constitucional nº 115 elevou a proteção de dados pessoais a direito fundamental explícito na Constituição, consolidando normativamente o tema em patamar constitucional. Esse movimento não apenas alinhou o Brasil a regimes internacionais, mas também reconheceu os dados como recurso estratégico em disputas de soberania e economia política global. A trajetória, portanto, revela um processo em que mecanismos de consumo, diretrizes regionais, legislação de transparência e direitos digitais se rearticularam até compor o regime normativo da LGPD como a temos hoje. Nossa gramática da governança de dados emerge, assim, como um ponto de inflexão que não rompe com um percurso passado, mas o reorganiza em chave regulatória alinhada a conjuntura externa que procuramos abordar nos capítulos anteriores. Ao incorporar princípios de autodeterminação informativa e ao prever uma autoridade de controle, a lei buscou se alinhar às tendências internacionais, estabilizando ao mesmo tempo o regime de extração de dados, fornecendo previsibilidade para mercados digitais e legitimidade para fluxos transnacionais de informação. Nesse sentido, a LGPD respondia, na ocasião de sua implementação, à pressão estrutural de integração do Brasil no capitalismo de dados, no qual proteção e exploração caminham lado a lado, ambivalência típica - como procuramos evidenciar - do capitalismo da vigilância global.

Do ponto de vista de suas engrenagens, a LGPD se estrutura em torno de princípios normativos (art. 6º), bases legais (art. 7º), direitos dos titulares (arts. 18–22) e de uma autoridade regulatória específica (arts. 55-A e ss.), compondo uma arquitetura que busca simultaneamente previsibilidade e flexibilidade. O legítimo interesse do controlador (art. 7º, IX), é permanece o dispositivo mais controverso ao permitir tratamento de dados sem consentimento explícito, condicionando-o a avaliações de proporcionalidade e de impacto, cujo efetivo controle depende da capacidade técnico-institucional da ANPD (Bioni, 2021; Doneda, 2006). Essa abertura regulatória aproxima o arranjo brasileiro de modelos anglo-saxões[24], mas contrasta com o regime europeu do GDPR, que tende a impor critérios

[24] Nesses contextos, a ideia central é a de ponderar e equilibrar interesses em conflito — por exemplo, entre o direito fundamental à privacidade de uma pessoa e o interesse legítimo de uma empresa ou do Estado em tratar dados pessoais. No campo da proteção de dados, ele aparece sobretudo quando se trata do legítimo interesse como base legal para o tratamento de informações. Nesse caso, o controlador avalia se existe um interesse legítimo real e relevante (por exemplo, segurança do sistema, prevenção de fraudes, melhoria de serviços), se o tratamento é necessário para alcançar esse interesse (não há alternativa menos intrusiva), se os direitos e

mais restritivos ao interesse legítimo (Bygrave, 2020). No Brasil, essa cláusula tornou-se um ponto de inflexão, permitindo tanto a inovação no setor privado quanto a expansão de margens de discricionariedade que podem ser capturadas por grandes plataformas. Outro eixo sensível para a literatura do campo está no direito à revisão de decisões automatizadas (art. 20), que responde a debates internacionais sobre explicabilidade algorítmica (Floridi, 2017). A previsão normativa traduz uma demanda de *accountability* frente à opacidade dos sistemas de *machine learning*, convivendo com limitações derivadas, por exemplo, de propriedade intelectual. Nesse sentido, os direitos positivados funcionam como técnicas de veridicção: criam zonas de visibilidade parcial, permitindo algum escrutínio público, mas também consolidando classificações e hierarquias próprias do capitalismo de dados (Zuboff, 2019).

A experiência brasileira com a LGPD revela como a proteção da privacidade foi incorporada a um campo normativo global que traduz direitos em parâmetros de conformidade regulatória. Elaborada feita à imagem e semelhança da GDPR, a LGPD estabelece um regime jurídico que equilibra o discurso da autodeterminação informativa com exigências de governança corporativa e gestão de riscos, representando, conforme discutido no Capítulo 2, a consolidação de uma racionalidade de *compliance* neoliberal, na qual o Estado se reconfigura como gestor da confiança e mediador de responsabilidades. A proteção da privacidade, nesse contexto, é convertida em um instrumento de legitimação de práticas que se ajustam a padrões internacionais de segurança, sustentáculos, em última instância, de uma economia global dataficada, conforme tratamos na seção 2.1.

A crítica de Couldry e Mejías (2019) ao colonialismo de dados permite compreender essa dinâmica como parte do processo mais amplo de apropriação da privacidade como recurso. Ao reconfigurar o sujeito de direito em sujeito de dados, o regime global de proteção transforma a privacidade em dispositivo de governança: o indivíduo torna-se responsável por gerir seu próprio risco informacional, enquanto o Estado atua como certificador moral da conduta corporativa, reforçando o argumento de que a governança neoliberal não elimina o poder soberano, mas o distribui em mecanismos de autorregulação e compliance que internalizam o controle. Por fim, a experiência brasileira sugere que o regime de proteção de

liberdades fundamentais do titular não prevalecem sobre esse interesse (aqui entra a ponderação). Bygrave (2020) e Edwards (2018) destacam que práticas correlatas, chamadas de *balancing test*, são altamente contextuais, dependendo de critérios interpretativos, e podem favorecer margens de discricionariedade regulatória — abrindo espaço tanto para inovação quanto para riscos de captura corporativa.

dados tende a legitimar a própria estrutura colonial da economia informacional. A implementação da LGPD manteve-se, nesse sentido, atrelada a uma lógica tecnocrática, voltada à adequação de processos.

Vale ressaltar que a promulgação da Lei Geral de Proteção de Dados foi recebida, por parte expressiva da sociedade civil e do setor privado, como um sinal inequívoco de modernização institucional e de maturidade regulatória. A adesão brasileira ao vocabulário técnico do compliance informacional foi celebrada como ingresso definitivo no "mercado global de dados", convertendo a privacidade em linguagem de competitividade e adequação normativa. Organizações empresariais e associações de tecnologia passaram a destacar a LGPD como marco de credibilidade internacional e de alinhamento às melhores práticas globais, enquanto think tanks e consultorias difundiram uma retórica de "governança responsável" que equiparava proteção de dados à eficiência administrativa e à confiança. Nessa narrativa, a privacidade é traduzida em termos de um requisito para participar legitimamente de cadeias globais de valor, recuperando a noção da governamentalidade neoliberal em termos de adequação e certificação.

Essa celebração revela a dimensão produtiva da privacidade como dispositivo econômico, no sentido foucaultiano do termo. A incorporação do Brasil ao circuito global da economia de dados não se dá apenas pela adoção de normas compatíveis com o Regulamento Geral de Proteção de Dados da União Europeia, mas pela aceitação da lógica que submete o valor jurídico à sua capacidade de gerar previsibilidade, confiança e capital reputacional. A LGPD, ao instituir figuras como o *encarregado, o relatório de impacto e a governança de riscos* (ver Anexo VII), internaliza a racionalidade da auto-responsabilização corporativa, transformando a proteção de dados em forma de gestão. Como já indicado no Capítulo 2, a governança neoliberal opera menos pela imposição de sanções do que pela produção de condutas conformes — um regime de governabilidade em que proteger significa demonstrar que se cumpre, e cumprir significa integrar-se ao fluxo.

A experiência brasileira, contudo, revela que tal promessa é atravessada por tensões constitutivas: enquanto o "mercado" comemora, as condições materiais de infraestrutura, transparência e fiscalização permanecem desiguais. A privacidade, transformada em capital de inserção internacional, nesse quadro parece reiterar um padrão colonial de dependência

normativa — uma inserção subordinada, em que a conformidade é celebrada como autonomia.

Em síntese, o Capítulo 4 procurou apontar para a inserção da LGPD num amplo conjunto normativo que configura um arranjo de governamentalidade tecnopolítica voltado à modernização da gestão pública, à conformidade regulatória e à inserção do Brasil em padrões internacionais de governança de dados, instituindo ciclos contínuos de melhoria e métricas em privacidade, convertendo a proteção de dados em tema de gestão pautado por desempenho e boas práticas. Esses instrumentos reforçam uma cultura de *compliance* informacional, a adesão a padrões globais é vista como indicador de maturidade administrativa. No interior dessa racionalidade tecnocrática, é confirmada a possibilidade de instrumentalização da privacidade como variável de desempenho e confiança, funcionando como dispositivo de legitimação em torno de uma perspectiva de governo do risco.

Considerações Finais

Esta tese partiu de um diagnóstico que recusa a narrativa linear da "erosão" da privacidade, propondo antes compreendê-la como dispositivo organizador de visibilidades, regulador de fluxos e produtor de sujeitos em um regime informacional atravessado por determinadas racionalidades. O argumento geral procurou demonstrar que a privacidade, longe de se extinguir, se reconfigura e é mobilizada para legitimar o pleno funcionamento de redes de circulação de dados, ao mesmo tempo em que oferece léxico jurídico-político de proteção de direitos. Essa dupla condição é interpretada, então, como mecanismo de governo cuja eficácia reside precisamente em operar entre promessas de salvaguardas e técnicas de legitimação.

Nosso Capítulo 1 foi dedicado a reconstruir criticamente a noção de segurança como tecnologia de governo, tomando como referência a contribuição de Michel Foucault. Nesse quadro, o risco torna-se operador central, por meio do qual o governo das populações pode ser racionalizado, projetando intervenções preventivas e modelando comportamentos em face do imprevisível. Essa abordagem nos permitiu sugerir que a vigilância pode ser pensada em termos de matriz normalizadora de governo, na medida em que se capilariza em parte integrante das rotinas administrativas, das infraestruturas de mobilidade, dos circuitos de informação e dos mercados digitais, constitutiva, portanto, de uma forma de governamentalidade que organiza a circulação de pessoas, bens e dados como condição da liberdade contemporânea. A circulação torna-se um problema técnico de governo, demandando seu acompanhamento, modulação e, em muitos casos, restrição para que a própria ideia de liberdade seja preservada. Também procuramos destacar como a virada cibernética, ao longo da segunda metade do século XX, reorganizou saberes e práticas pela emergência de sistemas digitais, redes de informação e técnicas algorítmicas que implicaram em uma expectativa de controle que já não se baseia simplesmente na vigilância retrospectiva, mas na antecipação e prevenção de riscos futuros. Essa perspectiva se revelou crucial para compreender de que maneira a privacidade não pode ser tratada como simples contrapeso à vigilância. Ao fornecer léxicos jurídicos e institucionais — direitos, garantias, autorizações — a privacidade participa da tradução das incertezas em padrões auditáveis. É justamente essa capacidade de converter tensões sociais em categorias mensuráveis e verificáveis que faz da privacidade um elemento profundamente funcional ao governo das circulações.

O Capítulo 2 procurou deslocar essa reflexão para o plano da arquitetura institucional da governança de dados, sob o marco do capitalismo da vigilância. Ao examinar as normas e instituições, sugerimos que a proteção de dados e a regulação da privacidade não necessariamente correspondem a obstáculos a um mercado voltado à captura e coleta de dados, mas como componentes internos incontornáveis de seu funcionamento. A regulação se apresenta como um campo de disputa, onde diferentes atores negociam fronteiras de uso, circulação e apropriação da informação. Nesse processo, ganha relevância a noção de governança que descreve como padrões técnicos, certificações, decisões de adequação e cláusulas contratuais tornam-se mecanismos centrais para viabilizar a circulação internacional de dados. Ao invés de um cenário de homogeneização regulatória sob um único modelo — como seria o caso se o Regulamento Geral de Proteção de Dados da União Europeia tivesse imposto uma uniformidade global — o que se observa é uma dinâmica de interoperabilidade performática. Caminhamos, a partir daí, para a discussão da fragmentação regulatória como uma tecnologia de governo que, por sua vez, produz condições para que cada contexto ajuste a proteção de dados às suas determinadas prioridades, ao mesmo tempo em que permanece um léxico universal de direitos fundamentais que confere legitimidade ao processo. Em outras palavras, a fragmentação não impede a circulação global de dados, a viabilizando na medida em que modula níveis de proteção de acordo com uma rede complexa de atores e mercados, no interior do qual provedores de tecnologia, certificadoras, órgãos reguladores e organizações internacionais desempenham papéis complementares.

O Capítulo 3 recuperou a hipótese do *dispositivo privacidade* ao acompanhar a passagem de um enquadramento liberal — no qual a privacidade figurava sobretudo como direito negativo, uma barreira à intrusão — para um arranjo no qual ela passa a operar como mecanismo de subjetivação e gestão da vida. Essa passagem não representa substituição pura e simples: trata-se de uma reconfiguração na qual camadas permanecem ativas, ainda que articuladas agora a narrativas técnicas próprias de um regime informacional. Se, no registro liberal, a proteção era concebida como recuo defensivo, ancorado em garantias de não interferência, o que se observa no regime atual é a constituição de um campo de governo, no qual proteger implica produzir condições de circulação, estabelecer métricas de aceitabilidade, desenhar rotinas e documentações e, sobretudo, formar sujeitos capazes de se responsabilizar por riscos. É nesse ponto que consentimento, accountability e gestão de riscos assumem centralidade como elementos-chave da sustentação das engrenagens da captura dos

dados pelo mercado. O consentimento, nessa interpretação, se manifesta como uma tecnologia de legitimação do tratamento informacional, formalizando o encontro entre sujeitos e controladores de dados sob a gramática da escolha, ainda que o faça em ambientes marcados por assimetrias técnicas, informacionais e econômicas. A interpretação dessa dinâmica, tal como trabalhada no capítulo, busca reconhecer, ainda, sua função performativa: ele "faz existir" uma relação juridicamente pertinente ao mesmo tempo em que distribui responsabilidades, deslocando para o sujeito parte relevante do ônus de sua segurança. Essa performatividade reinscreve o direito fundamental na forma de ação administrável, na medida em que o consentimento é solicitado, registrado, revogado, renovado; deixa rastros, produz evidências e, nesse movimento, se integra a rotinas típicas do capitalismo da vigilância.

O capítulo procurou mostrar que a ênfase contemporânea na prestação de contas contribuiu ao adensar esse regime, abrindo espaço para instrumentos, padrões e procedimentos — políticas internas, registros de operações, avaliação de impacto, controles de acesso, logs, trilhas de auditoria, planos de resposta a incidentes. Ao sujeito dos dados, nesse sentido, é ofertada a promessa de segurança auto-mediada; ao controlador, atribui-se a obrigação de desenhar e comprovar salvaguardas. O risco, nesse contexto, hierarquiza o que deve ser feito, em qual ordem e com qual intensidade, sob quais justificativas e limites. Administrá a lógica do risco, portanto, é aqui o projeto. Essa administração, por sua vez, demanda dados sobre dados que medem propensões de dano, avaliam impactos, justificam exceções, (re)produzindo em consequência um circuito reflexivo em que os instrumentos de proteção legitimam a captura ininterrupta de mais informações *"para proteger melhor"*, relevando a falsa oposição entre a preservação da privacidade e a vigilância.

O efeito articulado desses três elementos é o deslocamento da autonomia: ela já não se exerce simplesmente como poder de exclusão (dizer "não"), mas sobretudo como performance de conformidade em ecossistemas moldados por políticas, termos, consentimentos estratificados, preferências granulares, centros de privacidade, dashboards de controle e outros artefatos. O sujeito "autônomo" é convocado a gerir preferências, compreender avisos, navegar em escolhas técnicas, acionar direitos com tempos e formatos predefinidos, interpretar respostas padronizadas. Longe de esvaziar direitos, buscamos evidenciar que esse rearranjo os reinscreve sob padrões, documentações e verificações, estabilizando a proteção como garantia institucional e, ao mesmo tempo, como técnica de normalização - aquilo que cumpre requisitos e se mostra auditável tende a ser reconhecido

como “adequado”, independentemente de suas eventuais externalidades. Aqui, um imperativo máximo de se atestar *conforme* cria a figura do grau de aceitabilidade, abrindo margens de cálculo para finalidades, bases legais e exceções.

O Capítulo 4 examinou a experiência brasileira de institucionalização da governança de dados como expressão de um processo mais amplo de modernização tecnopolítica, em que discursos de segurança, eficiência e inovação convergem para legitimar novos regimes de vigilância e regulação informacional. Reconstruindo o percurso histórico que vai das heranças autoritárias do aparato de inteligência do período militar à consolidação da Lei Geral de Proteção de Dados (LGPD), o capítulo demonstrou como a retórica da proteção da privacidade se entrelaça à racionalidade da segurança e à lógica neoliberal de gestão do risco. A partir da análise de normativas nacionais, argumentamos que a regulação brasileira da privacidade emerge não apenas como reação a ameaças externas, mas como componente de uma governamentalidade que combina transparência, controle e responsabilização individual.

A consolidação da LGPD e da Autoridade Nacional de Proteção de Dados (ANPD) foi compreendida como síntese desse processo: um marco que simultaneamente inscreve o Brasil na economia global dos dados e reafirma a dependência estrutural de infraestruturas e padrões transnacionais de *compliance*. O capítulo concluiu que a experiência brasileira expressa de forma paradigmática a ambivalência do dispositivo privacidade: entre a promessa de emancipação e a captura pela lógica do mercado e da segurança, torna-se um campo de disputa normativa e simbólica em que a privacidade funciona menos como barreira e mais como instrumento de governo. A institucionalização da governança de dados no Brasil, assim, não rompe com a tradição de vigilância, mas a reinscreve sob novos léxicos — de eficiência, inovação e transparência —, confirmando que o neoliberalismo digital-securitário opera tanto pela administração dos riscos quanto pela produção de sujeitos conformes à ordem informacional. Longe de pretender oferecer uma análise exaustiva do fenômeno, buscamos propor uma leitura crítica das condições de emergência dessa racionalidade, compreendendo a proteção de dados como um dispositivo de governo que simultaneamente afirma direitos e reorganiza as formas de sujeição. Assim, o caso brasileiro exemplifica como a privacidade se torna elemento estrutural de uma governamentalidade neoliberal, na qual a gestão da informação é tanto técnica de eficiência quanto de poder.

Com base nesse percurso, sintetizamos nossas contribuições em quatro frentes: ao analisar a privacidade como dispositivo, buscamos evidenciar seu papel de engrenagem na governamentalidade típica do capitalismo da vigilância, esclarecendo como direitos e exceções co-produzem subjetividades e infraestruturas. Isso permite ler o "equilíbrio" privacidade-segurança não como balança, mas como gramática de gestão do risco e da circulação. Procuramos, ainda, demonstrar que a consolidação contemporânea de proteções e salvaguardas é indissociável de percepções de crise que reconfiguram agendas (de Snowden à pandemia), e que a linguagem de direitos é, muitas vezes, o idioma operacional de arranjos tecnopolíticos que normalizam a exceção. Por último, procuramos deslocar o foco da homogeneização "à la GDPR" para uma governança por instrumentos e por interoperabilidades parciais, iluminando os modos pelos quais decisões de adequação, cláusulas padrão e certificações performam a compatibilidade entre regimes coerentes com a manutenção de suas assimetrias constitutivas.

A principal implicação teórica é reconhecer que, sob a virada cibernética, a privacidade torna-se um mecanismo de proteção administrada: ela garante direitos ao fixar processos, testes de proporcionalidade, bases legais e perímetros de uso; mas, ao fazê-lo, internaliza no próprio regime protetivo a gramática de exceções administrada (emergências, segurança pública, interesse público, pesquisa), convertendo a fronteira entre proteção e captura em margem de cálculo. No plano internacional, instrumentos e interoperabilidades despolitizam conflitos por meio de padrões técnicos e certificações; no plano doméstico, tratam cidadãos como perfis de risco, e a accountability amarra o titular à performance documentada do seu próprio "cuidado de si" informacional. Essa dialética não anula a relevância dos direitos; antes, mostra que a efetividade da proteção depende do contexto institucional e da correlação de forças que preenchem as cláusulas abertas do regime.

Dois limites merecem registro. Primeiro, a amplitude do objeto — que articula camadas teóricas, jurídicas, técnicas e geopolíticas — impôs escolhas de foco e de escala. Um percurso de inspiração genealógica buscou conectar níveis (global/nacional/infraestrutural), mas não pretendeu esgotar parâmetros nem a diversidade do fenômeno. Segundo, o recorte privilegiou marcos e viradas críticas, deixando para trabalhos futuros a estabilização de séries históricas e métricas de efeitos regulatórios. Esses limites, compreendemos, não enfraquecem o argumento central, mas delimitam um terreno a ser percorrido por investigações

subsequentes, nas quais a presente tese se propõe a funcionar como matriz analítica, mais do qualquer outra coisa.

Uma conclusão transversal que emerge é que proteger, hoje, significa governar sob e pelo risco. A privacidade, como dispositivo, faz convergir normas, práticas e infraestruturas que simultaneamente limitam e possibilitam usos, mediando relações entre Estado, mercado e sociedade por meio de padrões, verificações e exceções. Reconhecer essa dimensão, de nossa perspectiva, não é ceder ao cinismo, mas é condição para politizar escolhas técnicas e reorganizar a imaginação institucional. O caminho proposto não é o do abandono da proteção da privacidade, mas o de sua reconstrução estratégica. Ao final, esta tese sustenta que a privacidade e a governança de dados permanecem não como vestígio de uma esfera perdida, mas como campo de disputa, o qual decidirá se seguirá operando como interface da exceção ou se será reapropriada como tecnologia atenta à reorganização informacional em curso.

Os debates recentes, aos quais esta tese se reporta, sobre regulação da privacidade e da economia de dados evidenciam que o problema central não reside apenas na eficácia legislativa, mas na própria estrutura de poder que sustenta a lógica da dataficação. Procuramos identificar de que forma mesmo os marcos normativos interpretados como mais avançados — como o GDPR — permanecem ancorados em categorias que se mostram insuficientes para conter a escala e a opacidade dos sistemas de coleta e inferência de dados. A figura do "titular" e o princípio do "consentimento informado" não resistem à materialidade algorítmica dos processos de produção de perfis (Haggerty; Ericson, 2000), em que decisões automatizadas são tomadas a partir de inferências probabilísticas sobre sujeitos efetivamente ausentes, em particular quando nos referimos ao hemisfério sul. Nesse contexto, a regulação jurídica se converte em mecanismo de legitimação de práticas que ela mesma não é capaz de controlar, pois depende de um ideal de autonomia individual que se dissolve na arquitetura distribuída das infraestruturas digitais.

Nesse impasse, surgem tentativas de repensar o campo normativo a partir de princípios mais radicais, como o da descontinuidade semântica, formulado por Julie Cohen. Essa proposta procura impedir a fusão ilimitada de bases de dados e o uso cruzado de informações que extrapolem o contexto original do consentimento, em teoria buscando reconstruir a autonomia do sujeito informacional diante da integração total promovida pelas plataformas. Contudo, sua implementação prática confronta a própria arquitetura econômica

do capitalismo digital, no interior do qual a maximização de valor depende precisamente da continuidade semântica entre fluxos, sistemas e contextos, se chocando com uma contradição estrutural por excelência - a do núcleo político e econômico da sociedade contemporânea. Se a privacidade e a regulação ainda é o idioma por meio do qual se formula uma agenda de resistência, ela também é o campo onde se reproduzem as lógicas da sujeição. Reconhecer essa tensão exige deslocar o debate para uma crítica que reencontre as condições de possibilidade da autonomia e da reconstrução do comum.

Anexo I

Síntese: Privacidade vs. Dados Pessoais nos Marcos Normativos Internacionais

Período / Marco	Privacidade	Dados Pessoais	Observação
1948 – DUDH (ONU, art. 12)	Privacidade entendida como proteção contra interferências arbitrárias na vida privada, honra e reputação.	Não há referência a "dados pessoais" como categoria jurídica.	A noção é negativa: limite ao Estado, sem referência a bancos de dados ou fluxos informacionais.
1950 – CEDH (Conselho da Europa, art. 8)	Vida privada e correspondência protegidas como parte da dignidade humana.	Dados pessoais continuam ausentes como conceito.	Consolida privacidade como direito no contexto europeu, mas centrada na intimidade e comunicação.
1966 – PIDCP (ONU, art. 17)	Reforça a proibição de ingerências arbitrárias na vida privada.	Dados pessoais continuam ausentes como conceito.	Universaliza a linguagem da privacidade, mas não aborda riscos tecnológicos emergentes.
1980 – Diretrizes da OCDE	Desloca a privacidade para uma lógica de governança internacional.	Surge pela primeira vez a noção de dados pessoais identificáveis, com princípios de propósito, qualidade e segurança.	Primeira formalização de "dados pessoais" como objeto regulatório. Marca a virada informacional.

1990 – Res. 45/95 (ONU)	Privacidade vinculada à proteção contra abusos em arquivos informatizados.	Estabelece princípios sobre coleta e uso de dados armazenados.	A privacidade passa a ser mediada pelo tratamento de dados: a separação entre os conceitos começa a se estreitar.
1995 – Diretiva 95/46/CE (UE)	Privacidade mantida como valor central do regime europeu.	Dados pessoais ganham definição legal autônoma: qualquer informação relativa a pessoa identificada ou identificável.	A partir daqui, privacidade e dados pessoais se entrelaçam, mas com tratamento jurídico distinto.
2001 – Res. 1373 (ONU/CS)	A privacidade cede espaço à segurança no contraterrorismo.	Dados pessoais são instrumentalizados para vigilância e cooperação entre Estados.	A diferença ganha peso político: privacidade como obstáculo, dados como recurso estratégico.
2013 – Res. 68/167 (ONU, pós-Snowden)	Retoma a crítica à vigilância em massa, reafirmando a privacidade como direito humano.	Dados pessoais vistos como objeto da vigilância extraterritorial.	A tensão se explicita: privacidade como princípio, dados como matéria-prima da vigilância global.
2016 – GDPR (UE)	Privacidade reinterpretada em chave de proteção de dados.	Dados pessoais centralizam o regime regulatório, com bases legais, direitos e deveres	Convergência quase total: a privacidade é operacionalizada juridicamente como proteção de dados

		específicos.	pessoais.
2020s – Relatórios ONU sobre IA e biometria	Privacidade vinculada a riscos de discriminação, vigilância biométrica e IA.	Dados pessoais (biométricos, sensíveis, inferenciais) tornam-se categoria de alto risco.	A diferença se reduz: privacidade = campo normativo; dados pessoais = objeto técnico da regulação.

Anexo II

Marcos Internacionais da Proteção de Dados e Privacidade

Ano	Fonte	Marco	Impacto	Observações
1948	**ONU**	Declaração Universal dos Direitos Humanos (Art. 12)	Define a privacidade como parte essencial da dignidade humana.	Estabelece fundação normativa global, mas sem mecanismos de enforcement. Cria a tensão entre soberania estatal e universalidade dos direitos.
1950	**Conselho Europeu**	CEDH (Art. 8)	Reconhece direito à vida privada e correspondência.	Marca a centralidade da privacidade na tradição europeia de direitos humanos. Torna-se referência para jurisprudência transnacional.
1966	**ONU**	Pacto Internacional sobre Direitos Civis e Políticos (Art. 17)	Proíbe interferências arbitrárias ou ilegais.	Fortalece privacidade como limite à ação estatal. Não especifica mecanismos técnicos, permitindo interpretações diversas.

1980	**OCDE**	Diretrizes de Privacidade	Introduz princípios de propósito, proporcionalidade, segurança e responsabilidade.	Soft law voltado à fluidez de mercados e fluxos transfronteiriços. Dá início à governança por princípios em vez de regras rígidas.
1990	**ONU**	Res. 45/95 sobre arquivos informatizados	Define princípios de transparência, consentimento e proporcionalidade.	Primeira tentativa da ONU de regular bancos de dados informatizados. Reconhece riscos de novas tecnologias sem ainda oferecer enforcement.
1995	**UE**	Diretiva 95/46/CE	Primeiro regime de proteção de dados europeu com força legal.	Pioneira em harmonizar legislações nacionais. Estabelece a UE como polo de difusão normativa global.
2001	**ONU/CS**	Res. 1373	Amplia cooperação e vigilância internacional contra terrorismo.	Normaliza práticas de vigilância digital em nome da segurança. Reforça lógica securitária pós-11 de setembro.
2004	**Regional**	Rede Iberoamericana de Proteção de	Articulação regulatória latino-americana.	Espelha difusão europeia. Constrói coordenação regional

		Dados		baseada em padrões OCDE/UE.
2009	**Regional**	Resolução de Madrid	Proposta de padrão global de proteção de dados.	Consolida tentativa de criar gramática universal. Legitima soft law como instrumento de harmonização.
2013	**ONU**	Res. 68/167	Reação às revelações Snowden. Propõe supervisão independente.	Primeiro reconhecimento explícito da vigilância em massa como violação de direitos humanos.
2014	**ONU**	A/HRC/27/37 (Relatório ACNUDH)	Critica ausência de salvaguardas e transparência estatal.	Reforça papel do Conselho de Direitos Humanos como fórum de denúncia contra vigilância massiva.
2015	**ONU**	Mandato do Relator de Privacidade	Criação de relatoria específica sobre privacidade.	Institucionaliza a privacidade como agenda permanente na ONU.
2016	**UE**	GDPR (Reg. 2016/679)	Define novo padrão vinculante, com efeito extraterritorial.	Consolida hegemonia normativa da UE. Converte proteção de dados em requisito de inserção no capitalismo

				digital.
2017	**ONU**	Res. 71/199	Insta empresas a respeitarem a privacidade como direito humano.	Expande responsabilidade para além dos Estados. Pressiona corporações digitais transnacionais.
2017	**ONU**	A/HRC/39/29 – Big Data e Direitos Humanos	Denúncia de riscos estruturais da IA e biometria.	Reforça crítica às tecnologias emergentes como novas formas de governança desigual.
2018	**ONU**	Compêndio de Boas Práticas em Biometria	Define limites éticos no contraterrorismo.	Mostra tensão entre inovação tecnológica e salvaguardas mínimas de direitos.
2019	**ONU**	Roadmap para Cooperação Digital	Inclui dados como eixo da transformação digital sustentável.	Coloca a privacidade no centro da agenda de desenvolvimento digital global.
2019	**ONU**	Resolução 42/15	Regulação de IA e biometria com base em direitos humanos.	Reforça a necessidade de alinhamento entre inovação e proteção.
2020	**ONU**	A/HRC/43/29 (Secretário-Geral)	Relaciona privacidade a direitos sociais e	Expande a compreensão da privacidade para além

			econômicos.	da esfera civil-política.
2020	**ONU**	Res. 75/176	Exige salvaguardas em identidades digitais.	Reconhece riscos de projetos de identidade biométrica em contextos de vulnerabilidade.
2021	**ONU**	Global Pulse – Due Diligence	Ferramenta de avaliação de riscos do uso de dados.	Institucionaliza práticas de governança de dados dentro do sistema ONU.
2021	**ONU**	A/HRC/48/31 (Relatório sobre IA)	Recomenda moratória em reconhecimento facial.	Reconhece risco estrutural de discriminação algorítmica e controle biométrico.

Fonte: elaboração própria a partir de

Anexo III

Marcos da Proteção de Dados e Privacidade - Expansão (América Latina)

Ano	Fonte	Marco	Impacto	Observações
1994	**Brasil**	CF, Art. 5º, XII	Reconhece sigilo de dados e comunicações como direito fundamental.	Primeira inscrição constitucional na região, mas sem instrumentos específicos de enforcement.
2000	**Argentina**	Lei 25.326	Primeira lei nacional latino-americana reconhecida pela UE.	Marca a colonialidade normativa: adequação buscada como credencial econômica.
2002	**Regional**	Rede Iberoamericana de Proteção de Dados	Criação de fórum regional de autoridades e especialistas.	Canal de difusão de padrões europeus, pouca originalidade local.
2008	**Uruguai**	Lei 18.331 + URCDP	Legislação baseada na OCDE/GDPR, reconhecida pela UE.	Exemplo da busca por inserção nos fluxos transnacionais de dados.
2010	**Chile**	Reforma da Lei 19.628	Ampliação do escopo de proteção, consentimento e sanções.	Avanço importante, mas dependente de padrões internacionais.

2011	**México**	Lei Federal de Dados Pessoais em Posse de Particulares	Introduz proporcionalidade, finalidade e accountability.	Forte influência OCDE. Expande a privacidade como responsabilidade corporativa.
2012	**Peru**	Lei 29.733	Estabelece autoridade nacional de proteção de dados.	Expande garantias de acesso, retificação e cancelamento.
2013	**Colômbia**	Lei Estatutária 1581	Obriga entidades públicas e privadas a cumprir requisitos.	Insere tratamento de dados como campo regulado nacionalmente.
2014	**Brasil**	Marco Civil da Internet	Reconhece dados como direito fundamental online.	Vincula proteção de dados à governança da Internet.
2018	**Brasil**	LGPD	Define princípios, bases legais e cria ANPD.	Inspiração no GDPR. Ambivalência entre proteção e inovação.
2019	**Regional**	Guia RIPD	Orientações para implementação de leis nacionais.	Reforça a convergência regulatória regional em torno do modelo europeu.
2021	**Costa Rica**	Atualização da Lei 8968	Ampliação de garantias e fortalecimento da autoridade.	Moderniza a lei em consonância com o GDPR.

2022	**Argentina**	Revisão da Lei 25.326	Processo colaborativo com consulta pública.	Busca modernização para manter status de adequação.
2023	**Paraguai**	Lei 6534	Foco em interoperabilidade digital e proteção ao consumidor.	Mostra inserção tardia, sob lógica de integração ao mercado digital.

Fonte: elaboração própria a partir de

Anexo IV

Instrumentos Internacionais de Governança

Instrumento	Fonte	Padrão Normativo	Observações
UN Personal Data Protection and Privacy Principles (2018)	ONU (HLCM)	Diretrizes internas, não vinculantes.	Padronização no sistema ONU, mas sem força externa. Expressa governança organizacional.
OECD Guidelines (2013)	OCDE	Soft law, orientações de privacidade e fluxos transfronteiriços.	Influência global, mas desenhada para facilitar comércio digital.
Council of Europe Convention 108+ (2018)	Conselho da Europa	Convenção vinculante, com extensão extraterritorial.	Hard law internacional, mas restrita a Estados signatários.
GDPR (2016)	União Europeia	Hard law, aplicação extraterritorial.	Hegemonia normativa global. Converte proteção em requisito de competitividade.
African Union Convention (2014)	União Africana	Hard law sobre cibersegurança e proteção de dados.	Baixa ratificação limita eficácia. Demonstra assimetrias regionais.

APEC Privacy Framework (2015)	APEC	Soft law para interoperabilidade comercial.	Foco na facilitação do comércio digital, não em direitos fundamentais.
UNCTAD Digital Economy Reports	UNCTAD	Relatórios com recomendações.	Diagnostica assimetrias de capacidade regulatória.

Fonte: elaboração própria a partir de

Anexo V

princípios e tensões normativas do GDPR

Instrumento	Dimensão formal	Dimensão analítica
Art. 6º, I – Consentimento	Tratamento lícito se o titular der consentimento inequívoco para finalidades específicas.	Reconhece autodeterminação, mas o consentimento pode ser capturado por padrões de design obscuros ou contratos de adesão, reproduzindo assimetrias informacionais.
Art. 6º, II – Execução de contrato	Tratamento necessário para a execução de contrato no qual o titular seja parte.	Legitima coleta extensa em serviços digitais e plataformas globais, reforçando a figura do consumidor como gestor de riscos.
Art. 6º, III – Obrigação legal	Tratamento necessário para cumprimento de obrigação legal do controlador.	Reforça a legalidade formal, mas pode abrir espaço para exceções securitárias ou normativas amplas.
Art. 6º, IV – Interesses vitais	Tratamento necessário para proteger interesses vitais do titular ou de outra pessoa.	Abrange emergências médicas e situações de vida ou morte, mas pode expandir a vigilância biométrica em contextos de saúde.
Art. 6º, V – Interesse público / autoridade oficial	Tratamento necessário para execução de tarefa de interesse público ou exercício de autoridade oficial.	Justifica grandes cadastros estatais e monitoramento populacional. Legitima interoperabilidade transnacional em nome da governança.

Art. 6º, VI – Interesses legítimos	Tratamento necessário para interesses legítimos do controlador ou de terceiros, exceto quando prevalecerem direitos do titular.	Cláusula geral que amplia captura de dados sob a retórica da inovação e eficiência. Abre margem a forum shopping regulatório e ao poder de Big Techs.
Art. 9º – Dados sensíveis	Proíbe tratamento de dados de saúde, origem racial/étnica, opinião política, crença religiosa, vida sexual, salvo exceções (consentimento explícito, interesse público, medicina, trabalho).	Formalmente protetivo, mas cria exceções que permitem rastreamento sanitário e laboral. Subjetiva o indivíduo como paciente-risco ou trabalhador monitorado.
Art. 10 – Dados criminais	Tratamento só por autoridade pública ou se autorizado por lei da União/Estado-membro, com garantias adequadas.	Reforça vigilância estatal sobre antecedentes criminais. Pode institucionalizar bancos de dados transnacionais de segurança.
Princípios (art. 5º)	Estabelecem legalidade, finalidade, minimização, exatidão, limitação de armazenamento, integridade/confidencialidade e accountability.	Funcionam como gramática normativa europeia. Ao mesmo tempo que protegem direitos, também sustentam práticas de gestão de risco e burocracias de compliance.
Direitos dos titulares (arts. 12–22)	Direitos de acesso, retificação, apagamento (direito ao esquecimento), portabilidade, oposição, limitação e não sujeição a decisões automatizadas.	Fortalecem autonomia formal, mas transferem ao indivíduo a responsabilidade de exercer direitos complexos em face de algoritmos opacos. Refletem a figura do cidadão como gestor de si.

Deveres do controlador e processador (arts. 24–43)	Devem implementar medidas técnicas e organizacionais, manter registros, nomear DPO, realizar DPIA, notificar violações.	Privacidade tratada como gestão de risco e conformidade. Gera mercado de auditoria, certificações e consultorias.
Transferências internacionais (arts. 44–50)	Permitem transferências apenas com decisão de adequação, cláusulas contratuais padrão, regras corporativas vinculativas ou exceções específicas.	Consolida hegemonia normativa da UE. Privacidade como requisito de inserção nos fluxos globais de capital, reforçando colonialidade regulatória.
Segurança do tratamento (arts. 32–34)	Impõem medidas técnicas e organizacionais para garantir integridade, confidencialidade e disponibilidade; exigem notificação de incidentes em 72h.	Enquadram violações como falhas de governança. Estimulam protocolos técnicos padronizados e métricas de resiliência.
Códigos de conduta e certificações (arts. 40–43)	Permitem elaboração de códigos setoriais, selos e certificações como mecanismos de conformidade.	Privatizam parte da regulação e transformam a proteção de dados em mercado de reputação e auditoria.
Sanções (arts. 83–84)	Preveem multas até 20 milhões de euros ou 4% do faturamento global anual; sanções graduadas pela gravidade e cooperação.	Fortes no papel, mas calibradas para estimular conformidade sem inviabilizar mercados. Reforçam lógica de incentivo econômico.
Autoridades de proteção de dados (arts. 51–59)	Cada Estado-membro deve instituir autoridade independente; criam Comitê Europeu de Proteção de Dados (EDPB).	Institucionalizam rede transnacional de autoridades. Fortalecem a UE como centro de difusão normativa global.

Fonte: elaboração própria a partir de

Anexo VI

Cronologia da LGPD

Período	Marco normativo	Impacto	Observação
1970s–80s	RENAPE; PL 2.796/1980; imaginário tecnocrático de centralização	Tentativa de criar cadastro nacional centralizado; reação parlamentar contra riscos de abuso.	Expressa herança autoritária e projeto de governança informacional centralizada. Mostra resistência inicial à concentração de dados, mas sem articular proteção como direito.
1988	Constituição Federal (art. 5º, X, XII, LXXII)	Reconhece privacidade, sigilo de comunicações e habeas data.	Marco inaugural de direitos informacionais no Brasil. Habeas data amplia instrumentos de defesa, mas permanece subutilizado. Ambivalência: protege, mas não regula tratamento por empresas.
1990	Código de Defesa do Consumidor (art. 43)	Garante acesso e correção de dados de consumo.	Inscreve proteção de dados em lógica de mercado. Privacidade aparece vinculada a relações de consumo, antecipando tensões entre direitos individuais e interesses econômicos.
2004–2005	Diretrizes do Mercosul sobre proteção de dados	Estimula harmonização normativa na região.	Primeira inserção explícita do Brasil em debates regionais. Influência indireta da Diretiva 95/46/CE. Reforça colonialidade normativa: importação de padrões europeus.
2011	Lei de Acesso à Informação	Amplia transparência e accountability.	Equilibra proteção com publicidade estatal. Tensiona privacidade e direito de acesso, evidenciando novos dilemas de governança informacional.
2014	Marco Civil da Internet	Estabelece princípios, direitos e deveres no ambiente digital.	Reconhece dados pessoais como direito fundamental online. Introduz regime de guarda de registros e segurança, articulando privacidade e vigilância.
2018	LGPD (Lei 13.709/2018)	Cria regime geral de proteção de dados; princípios, bases legais, ANPD.	Inspirada no GDPR, mas fruto de disputas locais entre sociedade civil, empresas e Estado. Ambivalência entre direito fundamental e estímulo à inovação.

2020	Dec. 10.474/2020 – criação da ANPD; entrada em vigor da LGPD	Estrutura regulatória nacional de proteção de dados.	ANPD nasce vinculada à Presidência, revelando fragilidade institucional. Conforma privacidade como campo de governança híbrida.

Fonte: elaboração própria a partir de CDC, LAI, MCI, LGPD.

Anexo VII

princípios e tensões normativas da LGPD

Instrumento	Dimensão formal	Dimensão analítica
I – Consentimento	“mediante o fornecimento de consentimento pelo titular”	Garante autodeterminação informativa em tese. Pode ser manipulado por contratos de adesão e interfaces opacas. Legitima extração de dados como 'escolha' do usuário. Convoca o titular a gerir riscos como indivíduo racional. Consentimentos globais padronizados reforçam a dependência de plataformas.
II – Obrigação legal ou regulatória	“para o cumprimento de obrigação legal ou regulatória pelo controlador”	Dá respaldo jurídico claro para usos entendidos como necessários. Normaliza exceções sob justificativa da lei (ex.: segurança pública). Amplia interoperabilidade entre órgãos estatais e privados. Produz sujeitos administrados por normas difusas. Reatualiza práticas autoritárias via legalidade formal.
III – Políticas públicas	“pela administração pública, para execução de políticas públicas [...]”	Possibilita programas sociais baseados em dados. Pode legitimar cadastros massivos e monitoramento populacional. Permite contratação de empresas de TI e parcerias público-privadas. Subjetiva o cidadão como 'perfil de risco' em políticas sociais. Abre fluxos de dados públicos a corporações transnacionais.
V – Execução de contrato	“quando necessário para a execução de contrato [...]”	Protege relações contratuais legítimas. Pode justificar coleta excessiva sob cláusulas contratuais. Alimenta ecossistemas de e-commerce, fintechs e telecom. Titular como consumidor que aceita rastreamento em troca de serviços. Plataformas globais

		moldam contratos padrão e práticas.
VI – Exercício regular de direitos	“para exercício regular de direitos em processo judicial, administrativo ou arbitral”	Salvaguarda acesso à justiça. Pode legitimar coleta e compartilhamento extensivo em litígios. Gera mercado de 'litigation analytics' e big data jurídico. Produz titulares como 'partes processuais' permanentemente rastreáveis. Integra dados judiciais a infraestruturas extrarregionais.
VII – Proteção da vida ou incolumidade	“para a proteção da vida ou da incolumidade física do titular ou de terceiro”	Dá legitimidade a emergências. Justifica monitoramentos biométricos e rastreamentos preventivos. Pode gerar mercado de biometria, wearables e vigilância médica. Titular como corpo administrado pela lógica da prevenção. Emergências sanitárias alimentam dependência de infraestruturas globais.
VIII – Tutela da saúde	“exclusivamente [...] por profissionais, serviços de saúde ou autoridade sanitária”	Protege integridade em contexto médico. Pode ser ampliada em crises (ex.: Covid-19) para rastreamentos massivos. Interesse potencial de healthtechs e seguradoras. Subjetivação como paciente-risco, monitorado continuamente. Dados de saúde circulam em cadeias globais de capital informacional.
IX – Legítimo interesse	“quando necessário para atender aos interesses legítimos do controlador [...]”	Exige teste de balanceamento (interesses x direitos). Funciona como cláusula geral de exceção. Amplia coleta em nome da inovação e da eficiência. Titular como gestor a quem cabe aceitar riscos em troca de serviços. Facilita forum shopping regulatório e captura por Big Techs.

X – Proteção do crédito	“para proteção do crédito”	Permite controle de endividamento e inadimplência. Amplia sistemas de scoring com efeitos discriminatórios. Titular como perfil de risco econômico. Conecta sistemas nacionais a cadeias globais de análise de crédito.
§3º – Dados de acesso público	“o tratamento [...] deve considerar a finalidade, a boa-fé e o interesse público”	Reforça limites ao uso discriminatório. Permite reuso amplo de dados tornados públicos. Abre espaço para a mineração de dados abertos por empresas. Titular transformado em 'informação pública' permanentemente acessível. Dados públicos brasileiros podem ser apropriados por plataformas estrangeiras.
Art. 11, §4º – Saúde (sensíveis)	“vedada a comunicação [...] de dados sensíveis referentes à saúde com objetivo de obter vantagem econômica”	Limita a mercantilização de dados sensíveis. Exceções permitem compartilhamento em certas condições. Reconhece pressão econômica sobre dados de saúde. Titular como corpo-mercadoria em disputa de regulação. Reforça a vulnerabilidade de países dependentes de infraestruturas de saúde digitais.
Princípios (art. 6º)	Listam critérios como finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação e accountability.	Gramática normativa aberta que permite flexibilidade. Podem reforçar direitos ou justificar eficiência e racionalização. Accountability reforça a cultura de compliance.
Direitos dos titulares (arts. 18–22)	Acesso, correção, anonimização, portabilidade, eliminação e revisão de decisões automatizadas.	Autonomia formal, mas responsabilidade deslocada para o indivíduo em ambiente de assimetria informacional. Subjetiva o cidadão como gestor de sua privacidade.
Deveres do controlador e operador (arts. 37–41)	Registros de operações (ROPA), encarregado (DPO), medidas organizacionais.	Produzem cultura de compliance documental. Evidências de conformidade superam o controle substantivo. Conformidade vira métrica auditável.

Transferência internacional (arts. 33–36)	Exige garantias adequadas, cláusulas-padrão ou decisão de adequação da ANPD.	Insere o Brasil em regimes transnacionais, subordinado a padrões eurocêntricos (GDPR). Privacidade como requisito de inserção em fluxos globais de dados.
Medidas de segurança (arts. 46–49)	Obrigam medidas técnicas e administrativas aptas a proteger dados pessoais.	Enquadram privacidade como gestão de risco. Transferem responsabilidades a protocolos técnicos e certificações. Incidentes vistos como falhas de governança, não abusos estruturais.
Boas práticas e governança (arts. 50–51)	Permitem códigos de conduta, selos e certificações reconhecidas pela ANPD.	Privatizam parte da regulação: associações e certificadoras passam a criar normas. Proteção convertida em mercado de conformidade.
Sanções administrativas (arts. 52–54)	Preveem advertências, multas e suspensão de atividades de tratamento.	Atuam como incentivo à adequação formal, moduladas por boa-fé e cooperação. Preservam continuidade do mercado, não freios absolutos à exploração.
ANPD (arts. 55-A a 55-K)	Órgão regulador com funções normativas, fiscalizatórias e sancionatórias.	Vinculada à Presidência, não é agência independente. Mostra fragilidade institucional diante de pressões, mas também convergência com padrões internacionais.

Fonte: elaboração própria a partir de LGPD

REFERÊNCIAS

ABDENUR, A. Brazil and cybersecurity in the aftermath of the Snowden revelations. In: DANE, F. (ed.). International security: a European-South American dialogue. Rio de Janeiro: Konrad Adenauer Stiftung, 2014. p. 229-283.

ALLEN, A. Unpopular privacy: what must we hide? Oxford: Oxford University Press, 2011.

___. Why privacy isn't everything: feminist reflections on personal accountability. Maryland: Rowman & Littlefield Publishers, 2003.

ARTIGO 19. Brasil: análise da estratégia de cibersegurança. São Paulo: Artigo 19, 2016.

AUGUSTO, A.; WILKE, H. "Racionalidade neoliberal e segurança: embates entre democracia securitária e anarquia". In: RAGO, M.; PELEGRINI, M. (orgs.). Neoliberalismo, feminismos e contracondutas: perspectivas foucaultianas. São Paulo: Intermeios, 2019.

BENOIT, Colin; RAAB, C. The governance of privacy: policy instruments in global perspective. Nova Iorque: Routledge, 2019.

BENNET, C. Regulating Privacy: Data Protection and Public Policy in Europe and The United States. Ithaca: Cornell University Press, 1992.

___. Regulating the Computer: comparing policy instruments in Europe and the United States. European Journal of Political Research, Exeter, 16 (5), 1988.

___. The Privacy Advocates: Resisting the Spread of Surveillance. Cambridge: MIT Press, 2008.

BIGO, D. "Rethinking Security at the crossroad of International Relations and Criminology". British Journal of Criminology, 2016, p. 1-19.

BIGO, Didier et al. After Snowden: Rethinking the Impact of Surveillance. International Political Sociology, v. 8, n. 2, p. 121–144, 2014.

BIGO, Didier; WALKER, R. B. J. Foucault and the Modern International. Millennium: Journal of International Studies, v. 1, n. 1, p. 83–106, 2007.

BIGO, Didier. The Future Perfect of Suspicion and Prediction as a Dispositive of Security Today? Security Dialogue, v. 37, n. 4, p. 395–422, 2006.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

____. Proteção de dados pessoais: funções e limites do consentimento. Rio de Janeiro: Forense, 2020.

____. Regulação e proteção de dados pessoais: o princípio da accountability. Rio de Janeiro: Forense, 2022.

BONDITTI, P.; NEAL, A.; OPITZ, S.; ZEBROWSKI, C. “Genealogy”. In: ARADAU, C.; HUYSMANS, J.; NEAL, A.; VOELKNER, N. (orgs.). Critical Security Methods: New frameworks for analysis. Abingdon: Routledge, 2015.

BOUSQUET, A. J. The scientific way of warfare: order and chaos on the battlefields of modernity. Nova Iorque: Columbia University Press, 2009.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado, 1988.

_____. Decreto n. 10.046, de 9 de outubro de 2019. Governança do compartilhamento de dados. Diário Oficial da União, Brasília, 10 out. 2019.

_____. Decreto n. 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d305.htm. Acesso em: 15 maio 2022.

_____. Decreto n. 8.771, de 11 de maio de 2016. Regulamenta a Lei n. 12.965/2014. Diário Oficial da União, Brasília, 12 de maio de 2016.

_____. Lei n. 12.850, de 2 de agosto de 2013. Define organização criminosa. Diário Oficial da União, Brasília, 5 ago. 2013.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, 24 abr. 2014.

_____. Lei n. 13.260, de 16 de março de 2016. Lei Antiterrorismo. Diário Oficial da União, Brasília, 17 mar. 2016.

_____. Lei n. 9.296, de 24 de julho de 1996. Regula a interceptação de comunicações telefônicas. Diário Oficial da União, Brasília, 25 jul. 1996.

_____. Medida Provisória n. 954, de 17 de abril de 2020. Dispõe sobre compartilhamento de dados de telecomunicações com IBGE. Diário Oficial da União, Brasília, 18 abr. 2020.

_____. CARTILHA DO PPSI. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. CARTILHA SOBRE FINALIDADES E HIPÓTESES LEGAIS. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. Estratégia Brasileira para a Transformação Digital – E-Digital. Disponível em: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf. Acesso em: 6 set. 2025

_____. Estratégia de Governança Digital 2016-2019. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/relatorio_de_avaliacao_da_egd_2019.pdf. Acesso em: 6 set. 2025.

_____. Estratégia de Governança Digital 2020-2023. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/historico. Acesso em: 6 set. 2025.

_____. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018. Brasília: Gabinete de Segurança Institucional da Presidência da República, 2015.

_____. Estratégia Nacional de Defesa. Brasília: Ministério da Defesa, 2008.

_____. GUIA DE BOAS PRÁTICAS LGPD. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. GUIA DE BOAS PRÁTICAS PARA IMPLEMENTAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. GUIA DE REQUISITOS E OBRIGAÇÕES QUANTO À PRIVACIDADE E À SEGURANÇA DA INFORMAÇÃO. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. GUIA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. GUIA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. GUIA OPERACIONAL PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação (LAI). Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. Lei nº 12.965, de 23 de abril de 2014. Institui o Marco Civil da Internet. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. Lei nº 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. MODELO DE POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. MODELO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO. Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025.

_____. Política Cibernética de Defesa. Brasília: Ministério da Defesa, 2012.

_____. PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023. Institui o Programa de Privacidade e Segurança da Informação (PPSI). Disponível em: Serviços e Informações do Brasil. Acesso em: 6 set. 2025

BRAUN, D. Exército prepara defesa cibernética da Copa das Confederações, 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/08/exercito-prepara-defesa-cibernetica-da-copa-das-confederacoes.html. Acesso em: 15 maio 2022.

BROWN, W. Nas ruínas do neoliberalismo: a ascensão da política antidemocrática no ocidente. São Paulo: Politeia, 2019.

BRUNO, F. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BRUNO, Fernanda. Rastrear, classificar, performar. Rio de Janeiro: Mauad X, 2013.

BRUNS, A. Filter bubble. Internet Policy Review, v. 8, n. 4, 29 nov. 2019. Disponível em: https://policyreview.info/concepts/filter-bubble. Acesso em: 2 fev. 2022.

BULL, H. The anarchical society: a study of order in world politics. Nova Iorque: Columbia University Press, 1977.

BYGRAVE, Lee Andrew. *Data Protection Law: Approaching Its Rationale, Logic and Limits.* Oxford: Oxford University Press, 2020.

BYGRAVE, Lee Andrew. *Data Privacy Law: An International Perspective.* Oxford: Oxford University Press, 2015.

CARR, E. H. Vinte anos de crise: 1919-1939. Uma introdução ao Estudo das Relações Internacionais. Brasília: Editora Universidade de Brasília, 2001.

CASTELLS, M. A Galáxia da Internet. Rio de Janeiro: Zahar, 2001.

CAVELTY, M. D.; WENGER, A. "Cyber security meets security politics: complex technology, fragmented politics and networked science". Contemporary Security Policy, 2019.

CHAMAYOU, Grégoire. *A sociedade ingovernável: uma genealogia do liberalismo autoritário*. São Paulo: Ubu Editora, 2020.

CHUN, Wendy. Updating to remain the same: habitual new media. Cambridge, MA: MIT Press, 2016.

COALIZÃO DIREITOS NA REDE. Carta em Defesa da Autoridade de Proteção de Dados Pessoais. Coalizão Direitos na Rede, 13 de Junho, 2018. Disponível em:

COHEN, Julie E. Surveillance vs. Privacy: Effects and Implications. In: GRAY, David; HENDERSON, Stephen E. (ed.). Cambridge Handbook of Surveillance Law. New York: Cambridge University Press, 2017. p. 455-469.

___. Between Truth and Power: the legal constructions of informational capitalism. Oxford: Oxford University Press, 2019.

___. What is privacy for. Harvard Law Review, Cambridge, v. 126 (7), 2013.

COMITÊ EXECUTIVO CONTRA O TERRORISMO DAS NAÇÕES UNIDAS (CTED). *Compendium of Good Practices on the Use of Biometric Data in Counter-Terrorism*. New York: United Nations, 2018. Disponível em: https://www.un.org/securitycouncil/ctc. Acesso em: 15 jul. 2025.

CONSELHO DE DIREITOS HUMANOS DAS NAÇÕES UNIDAS (ONU). *Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age (A/HRC/27/37)*. Geneva: United Nations, 2014. Disponível em: https://undocs.org/en/A/HRC/27/37. Acesso em: 15 jul. 2025.

CONSELHO DE SEGURANÇA DAS NAÇÕES UNIDAS (ONU). *Resolution 1373 (2001): Threats to International Peace and Security Caused by Terrorist Acts*. New York: United Nations, 2001. Disponível em: https://undocs.org/en/S/RES/1373(2001). Acesso em: 15 jul. 2025.

COSTA, Murilo Duarte; COCCO, Giuseppe. Capitalismo de vigilância e lutas algorítmicas / Surveillance capitalism and algorithmic struggles. Ponta Grossa – PR / Rio de Janeiro – RJ.

COULDRY, N.; MEJIAS, A. U. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject". Television & New Media, v. 20, n. 4, 2019.

DARDOT, Pierre; LAVAL, Christian. A nova razão do mundo: ensaio sobre a sociedade neoliberal. São Paulo: Boitempo, 2016.

DATA PRIVACY BRASIL. Relatórios e notas técnicas sobre pandemia, mobilidade e compartilhamento de dados. São Paulo: Data Privacy Brasil, 2020–2022.

DAY, R. The modern invention of information: discourse, history and power. Carbondale: Illinois University Press, 2001.

DEIBERT, R. Black Code: inside the battle for cyberspace. Oxford: Signal, 2013.

DILLON, Michael; REID, Julian. Global Liberal Governance: Biopolitics, Security and War. Millennium: Journal of International Studies, v. 30, n. 1, p. 41–66, 2001. DOI: 10.1177/03058298010300010501.

DONEDA, D. O Marco normativo de privacidade e proteção de dados está em debate. Ministério da Justiça, 15 de dezembro de 2010. Acesso em 06 de dezembro de 2024.

____, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

____; ZANATTA, R. Personality Rights in Brazilian Data Protection Law: a historical perspective. In: ALBERS, M., et al. Personality and Data Protection on the Internet. Cham: Springer, 2022.

____. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DUNNE, T.; HANSEN, L.; WIGHT, C. “The end of International Relations theory?”. European Journal of International Relations, v. 19, n. 3, 2013, p. 405-425.

DWYER, A. C. et al. “What can a critical cybersecurity do?”. International Political Sociology, v. 16, 2022.

ERIKSSON, J.; GIACOMELLO, G. “Who controls the Internet? Beyond the obstinacy or obsolescence of the state”. International Studies Review, v. 11, n. 1, 2009, p. 205-230.

FEENBERG, A. A Teoria Crítica de Andrew Feenberg: Racionalização democrática, Poder e Tecnologia. Brasília: UNB, 2010.

FOUCAULT, M. Em defesa da sociedade. Curso dado no Collège de France (1975-1976). Trad. Maria Ermantina Galvão. São Paulo: Martins Fontes, 2005.

FOUCAULT, Michel. Nascimento da biopolítica: curso dado no Collège de France (1978–1979). São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. Society must be defended: lectures at the Collège de France (1975–1976). New York: Picador, 2003.

____. Microfísica do poder. Rio de Janeiro: Graal, 2000.

____. O nascimento da biopolítica. Curso dado no Collège de France (1978-1979). Trad. Eduardo Brandão. São Paulo: Martins Fontes, 2008b.

____. Vigiar e punir: nascimento da prisão. 20. ed. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

____. Segurança, território, população. Curso dado no Collège de France (1977-1978). Trad. Eduardo Brandão. São Paulo: Martins Fontes, 2008.

____. História da sexualidade. Vol. I: a vontade de saber. 13. ed. Rio de Janeiro: Graal, 1999.

FRITSCH, S. "Technology and global affairs". International Studies Perspectives, v. 12, n. 1, 2011, p. 27-45.

FUCHS, Christian. Political Economy and Surveillance Theory. Critical Sociology, v. 36, n. 1, p. 163–196, 2010. DOI: 10.1177/0896920509347144.

GILPIN, R. War and change in world politics. Cambridge: Cambridge University Press, 1981.

GREENLEAF, Graham. Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. Privacy Laws & Business International Report, n. 170, p. 22–25, 2021.

HAGGERTY, Kevin D.; ERICSON, Richard V. *Policing the Risk Society.* Toronto: University of Toronto Press, 1997.

HARAWAY, D. Simians, cyborgs and women: The reinvention of women. Nova Iorque: Routledge, 1991.

____. "Situated Knowledges: The science question in feminism and the privilege of partial perspective". Feminist Studies, v. 14, n. 3, 1988.

HAYES, Ben. NeoConOpticon: The EU Security-Industrial Complex. European Security, v. 18, n. 4, p. 445–465, 2009.

HERRERA, G. "The politics of bandwidth: international political implications of global digital information network". Review of International Studies, v. 28, n. 1, 2002, p. 93-122.

HUI, Y. Tecnodiversidade. São Paulo: Ed. Ubu, 2020.

INTERNETLAB. Vigilância de comunicações no Brasil: mapa legal e institucional. São Paulo: InternetLab, 2017.

KEOHANE, R. O.; NYE, J. S. "Power and interdependence in the information age". Foreign Affairs, v. 77, n. 5, 1998, p. 81-94.

KOOPMAN, Colin. *How We Became Our Data: A Genealogy of the Informational Person.* Chicago: The University of Chicago Press, 2019.

KUNER, Christopher. The Internet and the Global Reach of EU Law. In: HOFMANN, Rainer; TIGNINO, Mara (ed.). International Law and the Internet. Oxford: Oxford University Press, 2020.

LATOUR, B. "Where are the missing masses? The sociology of a few mundane artefacts". In: BIJKER, W. E. (ed.). Shaping technology/building society: studies in sociotechnical change. Cambridge: MIT, 1992.

LEMKE, Thomas. Rearticulating the Concept of the Dispositive: Combining STS and an Analytics of Government. Critical Policy Studies, v. 2, n. 1, p. 124–135, 2008.

LEONARDI BRICALLI, I. Surveillance Capitalism in an Age of Neoliberal Rationality / Capitalismo de Vigilância em uma Era de Racionalidade Neoliberal.

LOS, Maria. "Theorizing Surveillance in a Post-Communist Society." In: Lyon, David (ed.). *Theorizing Surveillance: The Panopticon and Beyond.* London: Routledge, 2016. p. 78.

LYON, D. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique". Big Data & Society, v. 1, n. 2, 2014. https://doi.org/10.1177/2053951714541861

LYON, David. Theorizing Surveillance: the panopticon and beyond. Portland: Willan Publishing, 2006.

MAIONE, E.; RODRIGUES, T. "Genealogia e Agonismo como Metodologia nas Relações Internacionais: Reflexões a partir da Justiça de Transição". Revista Carta Internacional, v. 14, n. 1, 2019, p. 153-176.

MARIUTTI, E. B. “Guerra, complexidade e informação: Automação da percepção e os sistemas preditivos de vigilância”. Revista Superior de Guerra, v. 35, n. 74, 2020a, p. 117-137.

____. “Do individualismo possessivo ao indivíduo possuído: a dissolução do projeto liberal de construção do indivíduo moderno”. Texto para Discussão, Unicamp, IE, n. 393, 2020b.

MCCARTHY, D. R. (ed.). Power, Information Technology, and International Relations Theory: the power and politics of US Foreign Policy and Internet. Nova Iorque: Palgrave Macmillan, 2015.

MINDLE, G. B. “Liberalism, Privacy and Autonomy”. The Journal of Politics, v. 51, n. 3, 1989.

MORGENTHAU, H. J. “Modern Science and Political Power”. Columbia Law Review, v. 64, n. 8, 1964, p. 1386-1409.

MOROZOV, E. Big tech - A ascensão dos dados e a morte da política. São Paulo: Ubu, 2018.

MUMFORD, L. Tecnicas Autoritarias y Democracias. Ciencia, Tecnología y Sustentabilidad. El Escorial, julho 2004 [1964].

MURAKAMI WOOD, David. Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism.

NISSENBAUM, H. “Where computer security meets national security”. Ethics and Information Technology, v. 7, n. 2, 2005.

_____. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press, 2010

NYE, J. Power in a global information age: from realism to globalisation. Nova Iorque: Routledge, 2004.

_____. “The Regime Complex for Managing Global Cyber Activities.” *Global Commission on Internet Governance Paper Series*, no. 1, May 2014. Waterloo: Centre for International Governance Innovation (CIGI) / Chatham House.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *General Assembly Resolution 54/95: Cooperation between the United Nations and the Interpol.* New York: United Nations, 2000. Disponível em: https://undocs.org/en/A/RES/54/95. Acesso em: 15 jul. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris: OECD, 1980.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Revised edition. Paris: OECD, 2013.

O'NEIL, C. Weapons of math destruction: how big data increases inequality and threatens democracy. Nova Iorque: Crown Publishers, 2016.

PARISER, E. O filtro invisível: o que a internet está escondendo de você. Trad. Diego Alfaro. Rio de Janeiro: Zahar, 2012.

PARRA, H. "Abertura e controle na governamentalidade algorítmica". Ciência e Cultura, jan.-mar. 2016. Disponível em: http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252016000100013. Acesso em: 16 fev. 2022.

PARRA, H. Z. M.; ABDO, A. H. "Tendencias democráticas y autoritarias, arquitecturas distribuidas e centralizadas | Democratic and authoritarian tendencies, distributed and centralised architecture". LIINC EM REVISTA, v. 12, 2016, p. 335-350.

PASSETTI, E.; AUGUSTO, A.; CARNEIRO, B. S.; RODRIGUES, T. Ecopolítica. São Paulo: Hedra, 2019.

PEOPLES, C. "Technology, philosophy and international relations". Cambridge Review of International Affairs, v. 22, n. 4, 2009, p. 559-561.

QUJANO, Aníbal. Coloniality and modernity/rationality. Cultural Studies, v. 21, n. 2–3, p. 168–178, 2007. DOI: 10.1080/09502380601164353.

RAUHOFER, J. "Privacy is dead, get over it! Information privacy and the dream of a risk-free society". Information & Communications Technology Law, v. 17, n. 3, 2008.

REGAN, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill: The University of North Carolina Press, 1995.

RENÁ, Paulo. Direito, tecnologia e cultura digital: anotações sobre o Marco Civil da Internet. Brasília: Universidade de Brasília, 2014.

RODRÍGUEZ, Pablo. Extrálogo. In: TIQQUN. La hipótesis cibernética. Buenos Aires: Hekht Libros, 2015.

ROTENBERG, M. "Fair information practices and the Architecture of Privacy". Stanford Technology Review, 2001.

ROUVOY, A.; BERNS, T. "Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação?". Revista Ecopós, v. 18, n. 2, 2015.

ROUVROY, A. O(s) fim(ns) da crítica: behaviorismo de dados versus devido processo. In: ALVES, M. A. S.; NOBRE, M. R. (orgs.). A sociedade da informação em questão – O direito, o poder e o sujeito na contemporaneidade. 1. reimp. Belo Horizonte: Editora D'Plácido, 2020. p. 15-46.

SALTER, M. B.; WALTERS, W. "Bruno Latour Encounters International Relations: An Interview". Millennium: Journal of International Studies, v. 1, n. 23, 2016.

SANTOS, L. G. Politizar as novas tecnologias: O impacto sociotécnico da informação digital e genética. São Paulo: Editora 34, 2011.

SANTOS, R. E. "Governamentalidade algorítmica e subjetivação: sobre os riscos da construção de subjetividades em um mundo digital". REVES - Revista Relações Sociais, v. 2, n. 1, 2019. Disponível em: https://periodicos.ufv.br/reves/article/view/3234. Acesso em: 20 ago. 2021.

____. A Informação após a Virada Cibernética. In: Revolução Tecnológica, Internet e Socialismo. São Paulo: Ed. Fundação Perseu Abramo, 2003.

SCHEUERMAN, W. "Realism and the critique of technology". Cambridge Review of International Affairs, v. 22, n. 4, 2009, p. 563-584.

SHAMIR, Ronen. The Age of Responsibilization: On Market-Embedded Morality. Economy and Society, v. 37, n. 1, p. 1–19, 2008.

SILVEIRA, S. A. Democracia e os códigos invisíveis – como os algoritmos estão modulando comportamentos e escolhas políticas. Edições Sesc, 2019.

SILVEIRA, Sérgio Amadeu da. Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Editora Elefante, 2020.

SIMITIS, S. Reviewing Privacy in an Information Society. 1987.

SIMMONS, B. "Preface: international relationships in the information age". International Studies Review, v. 15, n. 1, 2013, p. 1-4.

SOLAGNA, F. 30 anos de governança da Internet no Brasil: coalizões e ideias em disputa pela rede. 2020. Tese (Doutorado em Sociologia) Universidade Federal do Rio Grande do Sul, Porto Alegre, 2020.

SOLOVE, D. Privacy Harms. Boston University Law Review, Boston, 102, 2022.

STENGERS, I. No Tempo das Catástrofes. São Paulo: Cosac Naify, 2015.

STEVENS, T. "Global Cybersecurity: New Directions in Theory and Methods". Politics and Governance, v. 6, n. 2, 2019.

____. Cyber Security and the Politics of Time. Cambridge: Cambridge University Press, 2016.

TELES, E. "A governamentalidade algorítmica e subjetivizações rarefeitas". Kriterion, v. 59, n. 140, maio-ago. 2018. Disponível em: https://www.scielo.br/j/kr/a/PQTcJnpCGrP7PD5TrXKWzZm/abstract/?lang=pt. Acesso em: 26 set. 2021.

UNIÃO EUROPEIA. *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 (General Data Protection Regulation – GDPR).* Official Journal of the European Union, L 119, 4 May 2016

VAN DIJK, J. The Platform Society: Public Values in a Connective World.

VAN MUNSTER, R.; SYLVEST, C. "Reclaiming nuclear politics? Nuclear realism, the H-bomb and globality". Security Dialogue, 2014.

WACQUANT, Loïc. Três etapas para uma antropologia histórica do neoliberalismo realmente existente. Sociologia & Antropologia, v. 7, n. 1, p. 147–170, 2017.

WALTERS, William. *Some Critical Notes on "Governance"*. Studies in Political Economy, v. 73, p. 27–46, Spring/Summer 2004.

WALTERS, William. *Governmentality: Critical Encounters.* London; New York: Routledge, 2012.

WALKER, R. B. J. "Lines of Insecurity: International, Imperial, Exceptional". Security Dialogue, v. 37, n. 1, 2006.

WALTZ, K. N. Man, the state, and war: a theoretical analysis. Nova Iorque: Columbia University Press, 2001.

WEISS, C. "Science, technology and international relations". Technology in Society, v. 27, 2005, p. 295-313.

WENDT, A. Social theory of international politics. Cambridge: Cambridge University Press, 1999.

WEST, S. Data capitalism: Redefining the logics of surveillance and privacy.

WESTIN, A. Privacy and Freedom. Nova Iorque: IG Publishing, 2019.

WILLIAMS, M. C. "In the beginning: The International Relations enlightenment and the ends of International Relations theory". European Journal of International Relations, v. 19, n. 3, 2013, p. 647-665.

WINNER, L. "Do artifacts have politics?" In: The Whale and the Reactor: a search for limits in an Age of High Technology. Chicago: The University of Chicago Press, 1986.

WINNER, Langdon. Do Artifacts have Politics? In: KAPLAN, David (ed.). Readings in the Philosophy of Technology. Lanham, MD: Rowman & Littlefield Publishers, 2009. p. 251–263.

MURAKAMI WOOD, David. "Beyond the Panopticon? Foucault and Surveillance Studies." In: LYON, David (ed.). *Theorizing Surveillance: The Panopticon and Beyond.* London; New York: Routledge, 2006. p. 245–247

ZANATTA, R. A proteção de dados entre leis, códigos e programação. in: DE LUCCA, N., et al. Direito e Internet: Marco Civil da Internet. São Paulo: Quartier Latin, 2015. p. 447 - 470.

ZUBOFF, S. “Big other: capitalismo de vigilância e perspectivas para uma civilização de informação”. In: BRUNO, F. et al. (orgs.). Tecnopolíticas da vigilância: perspectivas da margem. São Paulo: Boitempo, 2018, p. 17-68.

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

____. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.