Economia de Dados: conceitos, sistemas de mensuração e políticas em países selecionados e no Brasil

Economia de Dados: conceituações, sistemas de mensuração e políticas no Brasil

Nota Técnica 5

Marcelo G. P. Matos

Rio de Janeiro, junho de 2024

Coordenação

Marcos Dantas, José Eduardo Cassiolato e Helena M. M. Lastres

REDESIST
Rede de Pesquisa em Sistemas Produtivos e Inovativos

Centro Internacional CELSO FURTADO de Políticas para o Desenvolvimento
The International CELSO FURTADO Center for Development Policies

www.redesist.ie.ufrj.br

www.centrocelsofurtado.org.br

Apresentação

Esta nota técnica é resultado do projeto de pesquisa "Medição da Economia de Dados: um estudo de caso sobre o Brasil" realizado pela Rede de Pesquisa em Arranjos e Sistemas Produtivos e Inovativos Locais (RedeSist), através do Centro Internacional Celso Furtado de Políticas para o Desenvolvimento (Cicef) com apoio do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet do Brasil (CGI.br).

O projeto identificou e avaliou criticamente as principais conceituações e respectivos sistemas de mensuração disponíveis na literatura nacional e internacional para medição da "economia de dados" e analisou as principais tendências vislumbradas a partir do exame das experiências de diferentes países, blocos e organismos multilaterais.

A pesquisa, realizada de junho de 2023 a junho de 2024, buscou primordialmente examinar e caracterizar o papel da "economia política de dados" contribuir para a compreensão do estado atual da mensuração e elaborar um panorama da Economia de Dados no Brasil, a partir da coleta de estatísticas relevantes sobre o estoque, fluxo e uso de dados e os principais produtores e usuários. Visou, ainda identificar e analisar os esforços dos diferentes Estados nacionais no enfrentamento dos vários desafios colocados e, em especial, visando alcançar a soberania digital. Isso num quadro de grandes transformações, crescentes desigualdades entre países e populações, ataques à democracia e conflitos militares num mundo, onde os interesses das finanças comandam e controlam a estrutura produtiva e os esforços inovativos do sistema produtivo e inovativo digital da grande maioria dos países e regiões do mundo.

Foram elaboradas um conjunto de nove Notas Técnicas disponibilizadas como Texto para Discussão nas páginas da RedeSist e do Cicef:

1) FALCÓN, M. L. Economia de Dados: conceito, mensuração e repercussões na agenda de políticas da União Europeia.
2) ARROIO, A. Economia de Dados na perspectiva das Organizações Multilaterais e nos (B)RICS: mitos, conceitos e sistemas de mensuração para informar políticas no Brasil.
3) LEMOS, C. Economia de Dados: abordagens conceituais, sistemas de mensuração e políticas na África, Ásia e Oceania.
4) BRITTO, J. Economia de Dados: conceitos e sistemas de mensuração nos EUA e Canadá.
5) MATOS, M. Economia de Dados: conceituações, sistemas de mensuração e políticas no Brasil.
6) CASSIOLATO, J. E.; GASPAR, W. Digitalização e Financeirização: imbricações, desafios e possibilidades.
7) LASTRES, H. M. M. et al. Mitos, colonialismo e outros desafios da Economia de Dados.
8) GONZALO, M.; BORRASTERO, C. América Latina y la Economía de Datos: definiciones, mediciones, temas de agenda e implicancias de política.

9) LIMA, S. J. et al. Medição da economia baseada em dados: impactos, desafios e oportunidades para o Nordeste brasileiro.

Como acordado no projeto de pesquisa, o exame crítico dos resultados obtidos a partir de tais contribuições gerou três artigos para publicação pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br)/Comitê Gestor da Internet do Brasil (CGI.br).

1) CASSIOLATO, J. E.; DANTAS, M.; LASTRES, H. M. M. Marco conceitual e analítico da Economia de Dados.
2) LASTRES, H. M. M.; CASSIOLATO, J. E.; DANTAS, M. Estado atual da conceituação e mensuração da Economia de Dados no Brasil.
3) DANTAS, M.; LASTRES, H. M. M.; CASSIOLATO, J. E. Panorama da Economia de Dados no Brasil nos anos 2020.

Os coordenadores

Marcos Dantas, José Eduardo Cassiolato e Helena Maria Martins Lastres

Sumário

Lista de Quadros, Figuras e Tabelas

1 Economia de Dados como elemento constituinte de uma Soberania Digital e eixo importante para o desenvolvimento

A economia de dados é um conceito ainda em franca construção, havendo diversas propostas, mais ou menos análogas, de conceituação e uma diversidade de propostas distintas de mensuração. A partir da apropriação crítica de diversos conceitos propostos na literatura internacional[1], a RedeSist propõe como orientadora da presente pesquisa a seguinte definição:

> A Economia de Dados refere-se ao valor econômico e estratégico derivado do aproveitamento dos dados disponíveis, bem como aos princípios, às práticas e políticas necessárias para sua gestão durante o ciclo produtivo que envolve geração, captura, armazenamento, custódia, processamento, análise e reuso de dados para os diversos setores da sociedade, incluindo empresas, governos e indivíduos. Além disso, a Economia de Dados abrange aspectos e processos relacionados à privacidade, segurança e ética no tratamento de dados.

Conforme tal definição, a economia de dados constitui uma parte, porém de crescente centralidade, dentro do escopo mais amplo da economia digital.

O fluxo central da economia dos dados começa com a geração de dados nas mais diversas esferas: (i) indivíduos e seus hábitos de consumo, suas redes de interação, seus interesses e opiniões expressas em redes digitais, suas finanças, sua condição de saúde e aspectos mais gerais de seu corpo, características e aspectos de seu lar, etc.; (ii) empresas e seus dados contábeis, contratos, bases de clientes, especificações técnicas, dados operacionais, recursos humanos, etc.; (iii) governos e os dados sobre orçamento e execução orçamentária, dados sobre os cidadãos e seu acesso a políticas públicas, etc.; (iv) instituições de ensino e pesquisa; (v) sensores que se tornam crescentemente presentes na esfera produtiva, nos produtos, na infraestrutura urbana e dentro dos lares. Como esta listagem, necessariamente incompleta, evidencia, dados são crescentemente gerados nas mais diversas esferas da sociedade, se tornando insumo fundamental para a organização da vida individual e da vida em sociedade.

Referindo à definição citada acima, merecem destaque as atividades de processamento e análise de dados. Neste escopo se destaca o grande poder disruptivo, ainda não bem apreendido, da inteligência artificial. Grandes avanços em termos da capacidade de circulação de dados e o desenvolvimento do poder computacional associado ao acesso a um imenso pool de dados de treinamento têm permitido avanços na aprendizagem de máquina (*Machine Learning*), impulsionando um crescimento exponencial da capacidade de modelos de inteligência artificial. Tecnologias emergentes como a computação quântica podem permitir novo salto. O potencial disruptivo da IA aponta tanto para perspectivas muito virtuosas, tendo em vista o possível impacto sobre a saúde, tecnologias limpas e eficientes, gestão pública e geração de riqueza, quanto para perspectivas muito viciosas, associadas ao risco de seu uso como arma em cenário de disputas geopolíticas, terrorismo, vigilância e eliminação de liberdades individuais, manipulação política e concentração abissal de riqueza, etc.

[1] Por exemplo Bean (2016), UNCTAD (2021), IDC (2022), entre outros.

Por fim, a definição acima traz em seu cerne a exploração econômica de dados. Sua monetização pode se dar através da venda de dados, da oferta de serviços relacionados com dados e da utilização de dados para melhorar as operações comerciais. De acordo com uma estimativa, em 2020 foram gerados aproximadamente 2,5 quintilhões de bytes de dados todos os dias[2]. O mercado global de dados foi avaliado em US$ 271,83 bilhões em 2022, sendo previsto um crescimento para US$ 307,52 bilhões de dólares em 2023 e para US$ 745,15 bilhões até 2030[3]. Serviços de computação em nuvem geraram receitas substanciais: a Amazon Web Services (AWS) registou receita de US$ 45 bilhões em 2020 e este valor quase dobrou em dois anos, chegando a US$ 80 bilhões em 2022[4]. Uma pesquisa recente prevê um crescimento médio de 10,5% do mercado global de *data centers* , passando de US$ 187,35 bilhões em 2020 para cerca de US$ 517 bilhões em 2030[5]. No que se refere ao mercado de serviços de IA, diferentes estimativas apontam para um valor atual de mais de US$ 240 bilhões, com projeções para 2030 que variam de US$ 740 bilhões a mais de US$ 1,8 trilhões[6].

Os riscos relacionados à segurança de dados crescem junto com a economia dos dados. O número de violações de dados e o volume de dados expostos continuam a aumentar. Em 2022, só nos Estados Unidos, foram registradas mais de 1800 violações de dados, expondo mais de 400 milhões de registos[7]. No Brasil foram registradas, em 2022, mais de 103 bilhões de tentativas de ataques cibernéticos[8].

A reboque, emergem regulamentações que buscam proteger os dados e as identidades digitais dos cidadãos, como a Lei Geral de Proteção de Dados da União Europeia e, no Brasil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD). Estas regulamentações emergem no contexto de uma crescente preocupação não só com a segurança de dados, mas, em perspectiva mais ampla, com a soberania digital.

1.1 Dimensões Críticas para a Soberania Digital

O conceito de soberania, derivado da palavra latina *superanus*, que significa superior, tem sua origem na concepção do poder de uma entidade governante de se autodeterminar livre de interferências externas. Proposto pelo filósofo francês Jean Bodin no século XVI, a teoria tradicional de soberania fazia alusão ao poder da autoridade governante de tomar e fazer valer suas decisões. No século XVIII, Rousseau reposiciona o conceito no escopo de uma soberania popular, de forma que o termo passa a ser crescentemente associado com os conceitos de democracia, estado de direito e territorialidade. Atualmente, a soberania é entendida como a

[2] https://www.domo.com/data-never-sleeps

[3] https://www.fortunebusinessinsights.com/big-data-analytics-market-106179

[4] https://www.statista.com/statistics/233725/development-of-amazon-web-services-revenue/

[5] https://www.alliedmarketresearch.com/data-center-market-A13117

[6] https://www.statista.com/statistics/941835/artificial-intelligence-market-size-revenue-comparisons/

[7] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[8] https://www.cnnbrasil.com.br/economia/brasil-precisa-com-urgencia-de-marco-de-ciberseguranca-e-soberania-digital-diz-fgv/

independência de um Estado em relação a outros Estados (soberania externa), bem como o seu poder supremo de comandar todos os poderes dentro do território do Estado (soberania interna). De forma associada, a soberania democrática engloba o direito dos cidadãos de exercerem a sua autodeterminação, fazendo uso dos seus direitos inalienáveis.

A ideia de um Estado soberano tem sido desafiada por duas linhas de discurso relacionadas, que ganharam preocupante trânsito em discursos políticos e acadêmicos: "ciber-excepcionalismo" e "governança multi-stakeholder da internet". O primeiro, se alinha com uma visão de que a crescente importância da internet implicaria na extinção da autoridade do Estado. A complexidade das responsabilidades envolvidas e o alcance global das redes não poderiam ser corretamente tratados no âmbito das jurisdições nacionais, além das dificuldades para responsabilização de indivíduos. Adicionalmente, os avanços no marco legal seriam muito lentos para darem conta da velocidade das inovações tecnológicas e do surgimento de novos modelos de negócio. Nesta perspectiva, o ciberespaço emergiria como um âmbito autônomo e independente da interferência dos governos (BARLOW, 1996; KATZ, 1997). Tais perspectivas ressoam atualmente em discursos acerca da pretensa independência e governança autônoma no âmbito das criptomoedas e modelos de gestão autônoma com o emprego de tecnologias de blockchain (PISTOR, 2020; CHOHAN, 2017).

A segunda das linhas de discurso mencionadas emerge nos anos 2000. A tónica não está nas deficiências dos Estados na regulação, mas nas funções diferentes e não soberanas que os Estados deveriam desempenhar no contexto de um ideal de regulação que vê a administração da Internet como uma tarefa dos que são diretamente afetados por ela. Se inspira no surgimento, no âmbito da comunidade tecnológica, de uma diversidade de processos descentralizados para o estabelecimento de normas, regras e procedimentos para manter e desenvolver a internet. Nesta perspectiva, uma governança autônoma se daria no contexto de uma estrutura difusa *multi-stakeholder*, baseada em princípios de abertura, inclusão, colaboração e tomada de decisão por consenso, que poderia dispensar a necessidade de uma autoridade central reguladora, cabendo ao Estado, nos moldes dos discursos ultraliberais, apenas garantir as condições institucionais básicas para uma eficiente auto-regulação (CHENOU, 2014; HOFMANN, 2016; RAYMOND; DE NARDIS, 2015).

Em direta oposição a tais discursos, a partir dos desafios trazidos pelas tecnologias digitais e a internet, se consolida e difunde uma diversidade de acepções de soberania digital e soberania de dados. A referência à soberania neste escopo ganha visibilidade no discurso político a partir de declarações do governo Chinês. Em 2016, na abertura da Segunda Conferência Mundial da Internet, o presidente chinês Xi Jinping pontua[9]:

> The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an

[9] https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html

> equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security.

Ao longo da última década, fica evidente como os discursos ciberlibertários mencionados acima não se sustentam perante os fatos. Pelo contrário, o âmbito digital é crescentemente reconhecido como uma dimensão central de necessária garantia das soberanias nacionais. Em primeiro lugar, em oposição a um ecossistema marcado por uma multiplicidade de atores relativamente autônomos em redes descentralizadas, a espaço digital é crescentemente dominado por um grupo muito pequeno e crescentemente poderoso de corporações que possuem o poder de exercer domínio sobre estrutural sociais fundamentais, como a criação e regulação de mercados, a comunicação e a circulação de informação, desafiando atribuições tradicionalmente associadas a um estado soberano. No centro de seu modelo de negócio figura a geração, coleção, armazenamento, processamento, distribuição, análise, entrega e exploração de dados. As Big Tech têm consolidado sua liderança em áreas críticas, como computação em nuvem, big data, inteligência artificial, IoT, etc. Alphabet (Google), Amazon, Facebook se consolidam como proprietárias de vastas e crescentes carteiras de dados e posicionam como principais fornecedores de serviços públicos e infraestruturas (MAZZUCATO et al. 2021).

Em segundo lugar, preocupações com a soberania nacional emergem de evidências concretas do potencial de uso de tecnologias digitais para comprometer a segurança de diferentes estados. Destaca-se o escândalo revelado por Edward Snowden em 2013, que evidenciou práticas de vigilância dos mais diferentes estados nacionais por parte de agências de inteligência dos Estados Unidos da América. Este episódio evidenciou o amplo poder de coleção, análise e controle de dados exercido por aqueles que dominam os meios técnicos e as infraestruturas críticas de funcionamento da internet. Na mesma linha se coloca o ataque cibernético à principal instalação nuclear do Irã em 2021, que desligou a usina e colocou em risco os próprios mecanismos de segurança contra acidentes radioativos[10].

Um estudo da Internet Society (2022) explorou as diferentes acepções de soberania digital e de dados e as medidas/iniciativas mobilizadas a partir destes entendimentos. O que se verificou foi uma diversidade de entendimentos mais ou menos bem definidos, que podem ser agrupados em quatro categorias de objetivos.

Em primeiro lugar, destacam-se as perspectivas que enfocam na segurança nacional e na capacidade de fazer cumprir a lei (defesa do Estado de Direito). Dentre as preocupações com a segurança nacional, são destacados os riscos de ataques cibernéticos e vulnerabilidade de dados online. Aponta-se para o risco de organizações criminosas e os agentes maliciosos roubarem dados sensíveis ou praticarem espionagem e explorarem as vulnerabilidades dos sistemas digitais para sabotar infraestruturas críticas, tais como o sistema financeiro, as redes de energia, as redes de transporte e os sistemas de saúde que dependem fortemente da tecnologia digital. Ademais, agências de inteligência dependem de ferramentas e dados digitais para os esforços antiterroristas.

[10] https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility

Objetiva-se que o Estado proteja o domínio digital dentro das suas fronteiras. Um exemplo, nesta direção são as iniciativas de "localização de dados", que impõem exigências de armazenamento e processamento local de dados e que, por outro lado, buscam limitar o armazenamento, movimentação e processamento de dados para áreas ou jurisdições específicas, tendo em vista o objetivo de limitar o eventual acesso por parte de agências de inteligência estrangeiras e agências comerciais a dados críticos da estrutura industrial e dados pessoais de seus cidadãos[11]. Em perspectivas mais radicais, como exemplifica bem o caso chinês, também têm sido observadas políticas que permitem o acesso legal à informações e dados particulares por parte das agências estatais, políticas que limitam os softwares e serviços que podem ser acessados na internet local ou determinam a forma como estes devem funcionar, que promovem o controle das principais infraestruturas de rede, como a atribuição de nomes e endereços de internet. As diretrizes de cibersegurança CERT-In da Índia estendem o controle do Estado à coordenação da hora da rede, exigindo que todas as entidades e servidores se liguem aos servidores NTP (Network Time Protocol) do governo[12].

Em segundo lugar, podem ser identificados objetivos relacionados à promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços, tendo em vista a crescente dominação por parte de empresas estadunidenses e crescentemente chinesas. As iniciativas usualmente se articulam com planos mais amplos de política industrial e de inovação, buscando promover a capacidade competitiva de empresas locais no escopo de uma estratégia mais ampla de digitalização da economia (BAUMS, 2016; BRIA, 2015). Um exemplo é a iniciativa Gaia-X, anunciada conjuntamente pela Alemanha e França em 2019 e que busca estabelecer uma alternativa aberta, segura e confiável para os principais provedores de serviços de computação em nuvem e que respeita os valores e padrões de proteção de dados europeus (BMBF, 2019)[13]. Estas iniciativas se alinham com a crescente força que ganha no discurso político o conceito de soberania de dados (SUMMA, 2020; DE LA CHAPELLE; PORCIÚNCULA, 2021). Iniciativas também se alinham com o imperativo de garantir e proteger direitos do usuário e do consumidor, ao estimular a oferta de serviços que respeitam as leis e normas locais, com destaque para os parâmetros de proteção de dados (Hill, 2014). A estas iniciativas, se articulam diversas políticas industriais e de inovação, que oferecem estímulos diretos para o desenvolvimento de empresas nos diversos segmentos relevantes, objetivando constituir players nacionais com significativa capacidade competitiva.

---

[11] Em 2015, a Rússia implementou uma série de leis de localização de dados, exigindo que as empresas de Internet armazenassem os dados pessoais dos cidadãos russos em servidores localizados na Rússia (Lee, 2016). A Índia tem considerado leis de localização de dados para exigir que as empresas armazenem os dados dos usuários indianos no país (Bailey e Parsheera, 2021). Também é notória, neste sentido, a proposta encabeçada pela Deutsche Telekom de criar um Sistema Schengen de Roteamento de Dados, de forma a garantir que dados que circulem dentro do espaço europeu passem por rotas e nós situados fisicamente dentro deste espaço (Glasze e Dammann, 2021).

[12] https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[13] Como tentativa de não perderem o mercado europeu, a IBM lançou em 2015 a *German Cloud* que foi abandonada em 2018. E mais recentemente, empresas como VMware, Oracle, Microsoft, IBM e AWS lançaram um produto chamado *Sovereign Cloud*, nuvem soberana, que promete fornecer serviços de computação em nuvem conformidade com as leis e regulamentos locais do contratante.

Em terceiro lugar, podem ser identificados os objetivos de promoção de autonomia dos usuários e de autodeterminação individual, tendo em vista seus diferentes papeis como empregados, consumidores e usuários de tecnologias digitais, produtores de dados e, sobretudo, detentores de uma identidade digital. Por um lado, iniciativas tem buscado avançar no estabelecimento de um marco legal e regulatório que proteja identidades digitais e dados particulares, com o protagonismo da União Europeia[14]. Por outro lado, ações têm promovido o desenvolvimento de tecnologias locais de encriptação e proteção e gestão pessoal de identidades e dados e modelos de negócio mais transparentes[15]. De forma articulada, identificam-se iniciativas associadas ao conceito de "consciência de dados" (*Datenbewusstsein*) e literacia digital que buscam promover uma educação digital emancipadora, conscientizando usuários dos riscos de desinformação e do modelo de negócios a partir da extração de dados para manipulação do comportamento via apresentação seletiva e induzida de conteúdos e anúncios publicitários (BMBF, 2019; FLORIDI, 2020; HÖPER; SCHULTE, 2021; BELLI; GASPAR, 2023).

Por fim, de forma pontual e subordinada a outros discursos, identificam-se perspectivas que sublinham a importância de proteção da identidade e diversidade sociocultural, promovendo a proteção do patrimônio cultural e a diversidade linguística. Nesta linha se mobilizam iniciativas de promoção da produção de conteúdo nacional, o fortalecimento de grupos nacionais de mídia, a valorização de conhecimentos dos povos originários, etc. (TAYLOR; KUKUTAI, 2016; RICAURTE, 2019; GOFF, 2022).

Diversas análises têm apontado para o risco de muitas das iniciativas mobilizadas em nome da soberania digital contribuírem para o rompimento com os pretensos princípios fundantes da internet enquanto espaço livre, confiável e globalmente integrado. Argumenta-se que políticas podem restringir o desenvolvimento e implantação de tecnologias de infraestrutura e protocolos, afetando gravemente a interoperabilidade. Também, se aponta que, para atender a exigências de rastreamento de conteúdos, os intermediários de infraestrutura teriam que se especializar e adaptar os seus serviços, causando prejuízo à natureza tecnologicamente neutra e de propósito geral da Internet. Sobretudo, agrumeta-se que o emprego de técnicas de filtragem e monitoramento de dados colocam em cheque a confidencialidade e a integridade da informação. Neste contexto a internet tenderia à fragmentação em redes regionais/nacionais parcialmente fechadas (POHLE; THIEL, 2019, 2020; INTERNET SOCIETY, 2022). Por outro lado, argumenta-se que tal contraste entre uma internet aberta e uma tendência de "fechamento" e fragmentação só faria sentido tendo as características da rede na virada do século como referência de comparação, ao passo que a rede mundial atualmente já é marcada por sistemas crescentemente dominados por grandes corporações e pela capacidade fortemente assimétrica de exercício de poder econômico e simbólico (ONDRÁŠIK, 2007; KLIMBURG, 2017; ZUBOFF, 2018; PESSANHA, 2020).

[14] https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/

[15] https://en.wikipedia.org/wiki/Data_sovereignty; https://en.wikipedia.org/wiki/Digital_self-determination

1.2 Soberania digital e desenvolvimento pela perspectiva do Sul

As perspectivas traçadas acima impactam de forma diferenciada os países centrais, sede de muitas das Big Techs e/ou de empresas de tecnologia de porte e amplitude relevante, e os países periféricos, também caracterizados como subdesenvolvidos. O conceito de colonialidade ajuda a contextualizar muitas das relações assimétricas que se estabelecem entre as socioeconomias desenvolvidas e periféricas.

A colonialidade tem em sua gênese classificações raciais e étnicas das populações e impõem o padrão da metrópole de modernidade e de racionalidade. Esta relação se reforça através de meios materiais e construção de mentalidades de inferiorização de modos de vida, saberes e epistemes dos territórios da periferia (QUIJANO, 1992; LASTRES; CASSIOLATO, 2017).

Silveira (2021) evidencia como a colonialidade em um cenário de capitalismo informacional, organizado em uma economia de dados neoliberal contribui para um "epistemicío"[16] que serve para consolidar um número de "não-questões":

> Primeiro, a dúvida sobre a crença de que as empresas e plataformas digitais são neutras e que não interferem em nosso cotidiano, exceto para nos servir. Segundo, a interrogação sobre a inexistência de consequências negativas locais e nacionais na utilização das estruturas tecnológicas das plataformas, uma vez que elas respeitariam os contratos. Terceiro, a avaliação de que as implicações sobre a coleta massiva de dados nos países centrais da plataformização tecnológica possuem os mesmos efeitos econômicos, políticos e socialmente moduladores que nos países periféricos. Quarto, a indagação sobre se seria possível apostar no avanço de uma inteligência computacional local, na soberania algorítmica e no conhecimento tecnológico como um bem comum livre. (p. 35)

Conforme salienta Cassino (2021), o "colonialismo de dados"[17] mobiliza as mesma práticas e mecanismos do colonialismo histórico, mas engendrando um novo tipo de apropriação: a apropriação da vida humana, por intermédio da captura de dados. Adiciona-se o risco de captura da própria capacidade de discernimento e exercício do livre arbítrio em uma circunstância de alteração comportamental impulsionado por sistemas de inteligência artificial.

Ademais, cabe sublinhar como esse processo apresenta dinâmicas e implicações distintas para os países centrais do capitalismo de plataformas e para os países periféricos como os Latino-Americanos. O Norte figura como produtor e exportador das tecnologias, recebendo remessas financeiras do exterior e beneficiando suas economias com os lucros obtidos por suas empresas, além de impulsionar as competências científicas e tecnológicas no escopo de seus sistemas nacionais de inovação. Uma significativa parcela das verbas do mercado publicitário brasileiro, que circulavam dentro do país e impulsionavam a premiada criatividade da publicidade nacional, agora fluem para as plataformas no exterior que impõem suas estruturas e métricas

[16] "A destruição de algumas formas de saber locais, à inferiorização de outros, desperdiçando-se, em nome dos desígnios do colonialismo, a riqueza de perspectivas presentes na diversidade cultural e nas multifacetadas visões do mundo por elas protagonizadas" (Souza Santos; Meneses, 2009, p. 183).

[17] Couldry e Mejias (2019)

para maximizar a extração de retorno financeiro[18]. Os dados gerados no Sul Global alimentam os modelos de aprendizado de máquinas nos países centrais e turbinam a lógica de extração de renda pela comercialização dos dados. Serviços crescentemente complexos, baseados em computação em nuvem e processamento de grande volume de dados, são vendidos como pacotes fechados para empresas e governos da periferia, constituindo uma fonte adicional de extração unidirecional de riqueza, além de constituir fonte adicional de absorção de dados estruturados.

> A fusão do ordenamento neoliberal com as teias de colonialidade sustentam a posição de eterno dependente das tecnologias criadas na matriz. (Silveira, 2021, p. 49)

Cabe destacar as formulações desenvolvidas no seio da escola estruturalista latino-americana, que evidencia como o subdesenvolvimento se funda essencialmente na forma de assimilação do progresso técnico dentro do sistema capitalista mundial. Tal difusão se dá por duas vias, a assimilação de produtos finais de consumo e a assimilação de processos produtivos.

A assimilação pela via dos produtos finais tem sua raiz no ímpeto de modernização da elite das sociedades periféricas, com uma diversificação da estrutura de demanda sem uma contrapartida na estrutura produtiva. Esta análise, baseada em um período histórico muito antes do advento da internet, se mostra absolutamente atual, ao se observar como que a mídia e as redes sociais induzem um padrão simbólico e cognitivo único, resultante dos próprios mecanismos de tais plataformas de reforço de diferentes modalidades de adicção.

Ademais, Furtado (1998) também sublinha como que a assimilação de tecnologias "importadas", que, além de impor uma transferência de excedente em contrapartida, também impõe a assimilação de parte de uma trajetória histórica de desenvolvimento alheia ao sistema nacional periférico.

Os bens e serviços produzidos em determinado sistema nacional trazem em suas características fundamentais os valores culturais moldados pelas classes hegemônicas dentro de tal Estado nacional. O papel de pioneirismo no progresso tecnológico das economias centrais traz consigo a possibilidade de impor os padrões de consumo, os padrões de comportamento e estrutura de valor destes. Isto passa a condicionar a estruturação do aparelho produtivo de outras economias, as quais se tornam dependentes.

> [...] a forma de utilização desse excedente, a qual condiciona a reprodução da formação social, reflete em grande medida o processo de dominação cultural que se manifesta ao nível das relações externas de circulação. (Furtado, 1974, p.80-81)

[18] Desde o pioneiros banners e pop-ups, passando por mídias e influenciadores, até a inteligência artificial e a realidade aumentada, observa-se um crescimento contínuo de destinação de verbas publicitárias para o meio digital, dominado por grandes corporações estrangeiras. A participação da internet no mercado publicitário nacional, saltou de 7,6% em 2014 para 35,7% (representando R$ 7,6 bilhões) em 2022, com tendência de expansão. O crescimento de sua participação no mercado se dá à custas da queda de participação sobretudo da televisão aberta e dos jornais, dominados por empresas de capital nacional, passando, respectivamente, de uma participação de 58,5% e 11,4% em 2014 para 41,7% e 1,7% em 2022 (https://www.meioemensagem.com.br/midia/cenp-meios-mercado-publicitario-brasileiro-cresceu-76-em-2022)

A colonialidade que está na raiz desta dependência cultural também se manifesta no escopo dos embrionários marcos legais e regulatórios. Concebidos e pactuados no contexto do sistema sociocultural e econômico dos países centrais para tratar de assuntos como privacidade, identidade digital e defesa da concorrência, trazem em sua gênese as prioridades elencadas no escopo destas sociedades e se baseiam no seu grau de desenvolvimento de competências científicas, tecnológicas e inovativas. Na melhor das hipóteses, os serviços "desterritorializados" das *Big Techs* respeitarão tais marcos legais e regulatórios, a despeito de potenciais impactos perniciosos sobre as economias periféricas, que possuem uma capacidade apenas hipotética de *enforcement* para fazer cumprir a legislação local[19].

Estas considerações se alinham diretamente com o que na seção anterior foi tratado sob o prisma de objetivo de promoção da soberania digital e de dados: a proteção da identidade e diversidade sociocultural, promovendo a proteção do patrimônio cultural e a diversidade. Neste sentido, o que é citado como uma preocupação de importância secundária nas tendências internacionais, merece ser aqui tratado como algo de fundamental relevância para a promoção de um padrão autônomo e soberano de desenvolvimento. Portanto, ao analisarmos as conceituações e propostas de medição, é fundamental considerar em que medida essas levam em conta e avaliam o potencial de sistemas algorítmicos tratarem de forma desigual e invisibilizarem grupos, comunidades e territórios, gerarem vieses discriminatórios e colocarem em risco outras epistemes do Sul.

A partir destas ponderações, delineia-se, na sequência, um referencial analítico para explorar as conceituações da economia de dados no Brasil e as perspectivas para sua mensuração, que busca avançar para uma perspectiva sistêmica desta economia e que leva em conta os diversos aspectos relacionados à soberania digital e de dados, no contexto de um país periférico no escopo do capitalismo de plataformas.

2 Definição de um Referencial Analítico

A fim de definir um referencial analítico para explorar o caso brasileiro, propõem-se a articulação de três dimensões complementares. A sequência da análise irá explorar em que medida e com que grau de completude as definições explícitas ou implícitas da economia de dados contemplam aspectos das seguintes duas dimensões.

Em primeiro lugar, parte-se da caracterização da cadeia de valor da economia de dados e do sistema produtivo e inovativo mais amplo no qual esta se insere. Nesta perspectiva, caberá averiguar em que medida as definições explícitas ou implícitas englobam e atribuem a devida importância a cada uma das diferentes etapas que contribuem para a geração de valor nesta economia: geração de dados no âmbito de sociedade, estado e mercado; sua armazenagem e

[19] O pensamento de Souza Santos (2007) se contrapõe à tendência homogeneizante da "monocultura do saber científico", sobretudo com a ascensão hegemônica do Consenso de Washington e do neoliberalismo nos anos 1990, que desqualifica outros conhecimentos e produz o que ele chamou de "epistemicídio", isto é, "a morte de conhecimentos alternativos" como forma de fortalecer o discurso de que não há alternativas.

custódia; sua captura e processamento; sua análise e produção de conhecimento; e as diferentes modalidades de consumo de dados e serviços e produtos associados.

Como referência para os diferentes nichos de atuação e os modelos de monetização a partir dos dados, o quadro 1 destaca os players no cenário internacional.

Empresas como o Facebook e o Google fornecem um serviço pelo qual os consumidores não pagam diretamente. Empresas como a Airbnb e a Uber, intermedeiam a oferta e a procura de um serviço e cobram uma taxa por esse serviço. Os provedores de conteúdo e serviços vendem conteúdo ou serviços digitais, mediante pagamento de assinatura ou pagamento por unidade, além das variantes "gratuitas" que se monetizam pela inserção de publicidade e outros modos. Varejistas intermediam a relação entre produtores e compradores e se remuneram a partir de percentual do valor das transações, além de também inserirem publicidade direcionada. Em todos estes casos, de forma principal ou complementar, os consumidores também pagam indiretamente através da "produção" de novos dados que serão monetizados no sistema e pela atenção dedicada à publicidade direcionada inseridas nas plataformas.

Quadro 1 - Nichos e principais players da Economia de Dados na esfera internacional

Nichos	**Firmas dominantes**
Mecanismo de busca	Google
Mídia Social/mensagem	Facebook, WhatsApp, WeChat
Plataforma de Economia de Compartilhamento	Uber, Airbnb
Provedor de conteúdos e serviços	Netflix, Venmo, Expedia
Varejo e marketplace	Amazon, eBay, Alibaba
Sistema Operacional	Microsoft, Apple, Google
Hardware de dados	Apple, Samsung, Cisco

Fonte: ONU (2019)

Empresas como Microsoft, Apple, Google, Apple, Samsung e Cisco desenvolvem sistemas operacionais, software e hardware que permitem a captura, o armazenamento, o processamento e a transmissão de dados. Muitas das Big Techs, como Amazon e Google participam de muitos dos elos da cadeia de valor dos dados, captando dados dos consumidores, organizando e analisando esses dados, extraindo informações úteis, partilhando-os com terceiros.

A perspectiva ampla de sistema produtivo e inovativo da economia de dados traz em seu núcleo os atores e processos centrais da economia de dados, mas que a situa em um contexto mais amplo da economia digital e explicita as interfaces do subsistema de produção e inovação com outros subsistemas e o contexto mais amplo. A figura 1 apresenta uma representação esquemática do sistema produtivo e inovativo da economia de dados.

A figura situa as atividades centrais da rede de valor da economia de dados no centro da figura. Em termos de formas de monetização, destacam-se:

- Venda direta de bancos de dados
- Serviços de customização/direcionamento baseados em dados (*data targeting services*): pontuação de crédito/gestão de riscos; serviços de estratégia de precificação dinâmica; publicidade direcionada, etc.
- Serviços de consultoria para tomada de decisões, inovação, personalização de serviços - previsão e prospecção da demanda; serviços de contratação; consultoria e gestão logística, etc.
- Produtos baseados em dados
- Taxa acesso/uso

Diretamente articulados às atividades propriamente da economia de dados, destacam-se atores da economia digital, como os serviços de telecomunicações de infraestrutura da internet, enquanto canal através dados e serviços digitais fluem, bem como a indústria produtora de uma gama diversificada de produtos/hardwares e serviços produtores/softwares.

Figura 1 - Economia de Dados no centro do Sistema Produtivo e Inovativo Digital ou Cibernético

Fonte: Elaboração pela equipe de pesquisa da RedeSist

Em perspectiva mais ampla, o sistema produtivo e inovativo cibernético se articula com um sistema de inovação, com diversos tipos de atores e funções, conforme a figura 2. Em torno do núcleo produtivo, destacam-se a criação de capacitações, pesquisa e serviços tecnológicos, as políticas de promoção e regulação e financiamento, a representação e a participação social, todos inseridos em um contexto geopolítico, econômico, social, cultural

Figura 2 - Sistema Produtivo e Inovativo Digital ou Cibernético em seu Contexto Amplo

Fonte: Elaboração pela equipe de pesquisa

Portanto, tendo em vista o referencial analítico para este estudo, cabe averiguar em que medida as definições explícitas ou implícitas contemplam o conjunto completo de atores e competências do Sistema Produtivo e Inovativo da Economia de Dados, tendo em vistas as implicações desta perspectiva sistêmica para a promoção e o desenvolvimento destas atividades econômicas no país (CASSIOLATO; LASTRES, 2005; CASSIOLATO et al. 2014; SZAPIRO et al., 2017; MATOS et al., 2017).

Em segundo lugar, busca-se adicionar à análise considerações de caráter eminentemente estratégico. Parte-se da discussão empreendida nas páginas acima acerca da soberania digital e soberania de dados, para averiguar em que medida as definições explícitas e implícitas trazem um reconhecimento da importância das diferentes dimensões relacionadas ao desenvolvimento e à soberania do país. De forma associada, será averiguado em que medida documentos e discursos de política e iniciativas comtemplam os aspectos críticos e eventuais soluções para os desafios à soberania digital ou até mesmo colocam esta em cheque. Conforme a análise empreendida acima, estas preocupações/objetivos podem ser sistematizadas em quatro grupos:

(i) Segurança nacional e defesa do estado de direito
(ii) Promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços
(iii) Promoção de autonomia dos usuários e de autodeterminação individual
(iv) Proteção da identidade e diversidade sociocultural, promovendo a proteção do patrimônio cultural, a diversidade, a valorização dos diversos grupos, comunidades e territórios e a valorização de epistemes próprias

3 O Sistema Produtivo e Inovativo da Economia de Dados Brasileiro

Objetiva-se aqui, passar da representação abstrata do sistema produtivo e inovativo da economia de dados para uma perspectiva aplicada ao Brasil. Portanto, busca-se identificar os diferentes atores e organizações que atuam e interagem com o sistema produtivo e inovativo da economia de dados no país. Para tal, cabe iniciar traçando um panorama dos atores existentes nos subsistemas principais. O quadro 2 parte das categorias propostas no quadro 1 acima, mas adota nomenclatura que melhor evidencia o papel de diferentes atores na economia de dados e inclui categorias não previstas pelos autores do quadro 1, tais como serviços de consultoria e de customização/direcionamento baseados em dados, tendo em vista a crescente importância de serviços prestados a empresas e governos nas áreas de inteligência artificial, IoT, etc., bem como os serviços financeiros.

Quadro 2 - Nichos de atuação na Economia de Dados e Panorama no Mercado Brasileiro

Atividades	Atores
Motores de busca	Domínio da Alphabet/Google com participação residual do Bing e DuckDuckGo. Ausência de empresas nacionais
Mídia social e mensageria	Predomínio das plataformas internacionais: Meta (Facebook, Instagram, WhatsApp) e da Alphabet (YouTube) com concorrência do TikTok, Twitter, Telegram. Alguns atores nacionais em nichos: Bliive; iCampus Social; Skoob; Winwe; Teckler; Pergunter; Fashion.me; Receitáculo; ProprietárioDireto; etc. [20]
Intermediação para comercialização de bens	Predomínio de plataformas internacionais: Mercado Livre (Argentina 13,1%); Amazon (EUA, 9%); Shopee (China, 6%). Forte presença de empresas nacionais: Magazine Luiza (5%); OLX (4,6%); Via Varejo (Casas Bahia e Ponto Frio, 2%); Lojas Americanas (1,7%) e ainda, com menos de 1%, Raia Drogasil; Fast Shop; enjoei; Carrefour; e inúmeros pequenos atores. [21]

[20] https://exame.com/tecnologia/confira-10-redes-sociais-que-foram-criadas-por-brasileiros/
[21] https://www.conversion.com.br/blog/relatorio-ecommerce-mensal/

Intermediação para provisão de serviços	Predomínio de plataformas internacionais em segmentos de mercado como transporte (Uber), locação de imóveis (Airbnb), turismo (TripAdvisor) etc. Forte presença de nacionais: Ifood, QuintoAndar, 99; Zé Delivery, Tem Açúcar?; 4Mãos; DogHero; Turbi; Yellow, MoObie; Rentbrella; Blimo; Happymoment; etc. [22]
Provedor de conteúdos com base em assinaturas	Predomínio de plataformas internacionais, como Netflix, Amazon Prime e Spotify. Forte presença de empreendimentos nacionais grandes e pequenos: Globoplay (9,96%), Telecine, Spcine Play, Looke, À La Carte, Lumine e PlayPlus, Viuzz, AFRO.TV, DarkFlix, OldFlix, Univer etc. [23]
Insumos informacionais e consultoria baseada em dados	Predomínio de plataformas internacionais. Presença de empresas nacionais importantes como, p. ex., Totvs
Serviços financeiros Precisa uma breve pesquisa	Bancos tradicionais nacionais com acesso digital: Itau, Bradesco, Banco do Brasil, Caixa Econômica Federal, etc. Bancos digitais nacionais: Nubank, Inter, C6 Bank, BTG Pactual, Mercado Pago e PagBank, etc.

Fonte: Elaboração própria

Um estudo do mercado da economia digital no Brasil em 2022 (ABES, 2023) revela um universo de 33.475 empresas de softwares e serviços associados, sendo 25,3% atuantes no desenvolvimento e produção, 35,3% na distribuição e comercialização e 39,3% na prestação de Serviços. Dentre as empresas de desenvolvimento e produção de softwares, o cenário é similar ao de serviços de IA, com 48,2% sendo microempresas (com até 10 pessoas ocupadas) e outros 45,4% pequenas empresas (10 a 99 pessoas ocupadas). Especificamente, no que se refere a serviços centrados em dados e IoT, o estudo não apresenta um número de empresas atuantes, tampouco sua distribuição por tamanho, nichos de atuação e localização. Contudo, é apresentado um panorama do mercado de "*Business Intelligence* e *Analytics Software*" (tabela 1) e produtos, softwares e serviços para IoT (tabela 2).

[22] https://publiconline.com.br/economia-compartilhada-abrir/

[23] https://www.terra.com.br/diversao/tv/como-as-plataformas-brasileiras-de-streaming-estao-buscando-um-lugar-ao-sol,25c09b44c1baf577988ed307d02d630809hr3lme.html; https://www.startse.com/artigos/streaming-plataformas-brasil/

Tabela 1 - Evolução do Mercado Brasileiro de Business Intelligence e Analytics Software (US$ Milhões)

Categoria da Tecnologia	**2019**	**2020**	**2021**	**2022**	**2022/2021**
Plataforma	823	1.030	898	1.051	17,0%
Aplicações	373	455	388	435	12,1%
Total	1.196	1.485	1.286	1.486	15,5%

Fonte: ABES (2023)

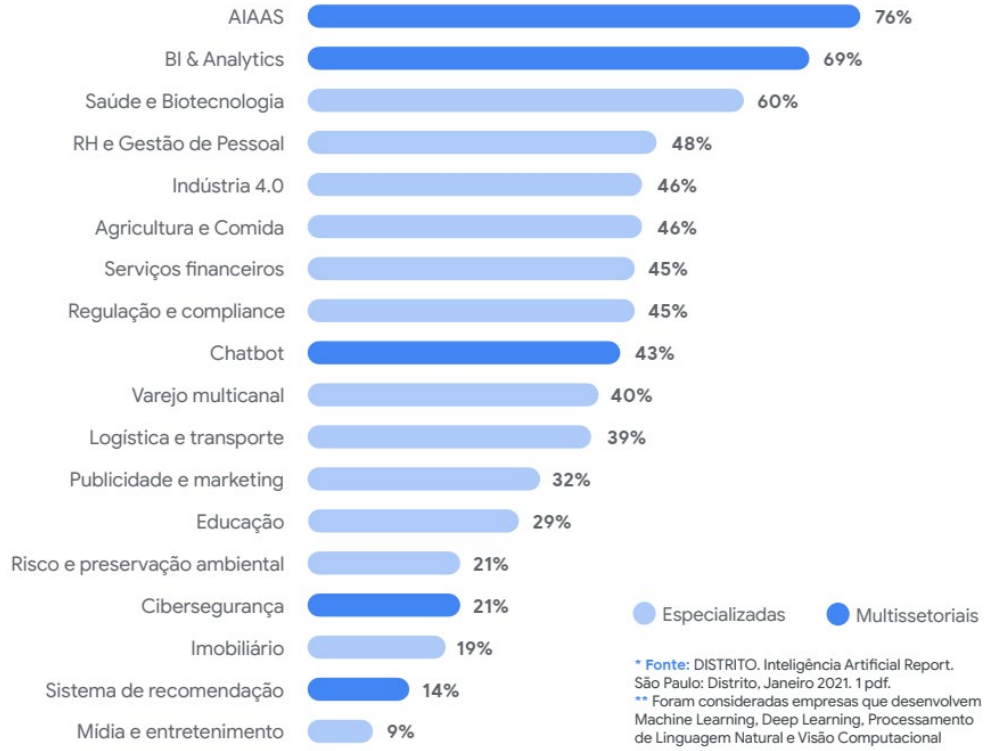
Tabela 2 - Evolução do Mercado Brasileiro de IoT (US$ Milhões)

Tecnologia	**2020**	**2021**	**2022**	**2022/2021**
Hardware/Conectividade	2.506	2.815	3.228	14,7%
Serviços	560	639	885	38,5%
Software	711	822	1.028	25,1%
Total	3.777	4.276	5.141	20,2%

Fonte: ABES (2023)

Outro estudo (Distrito, 2021) mapeou 702 empresas que trabalham e desenvolvem inteligência artificial no Brasil, englobando atividades de *machine learning*, *deep learning*, processamento de linguagem natural e visão computacional. O estudo mostra um mercado geograficamente bastante concentrado, com 92,7% das empresas nas regiões Sul e Sudeste do país; 51,9% no estado de São Paulo. A esmagadora maioria (85,7%) das empresas é voltada para soluções direcionadas para empresas (B2B). A figura 3 apresenta o percentual de empresas que atua com os diversos focos mapeados.

Figura 3 -Áreas de Atuação de Empresas Provedores de Serviços de Inteligência Artificial no Mercado Brasileiro



Fonte: Distrito, 2021

O perfil dominante é de pequenas empresas de criação recente. 70,2% das empresas possuem até 20 funcionários e 58,8% foram fundadas a partir de 2016. Destacam-se grande empresas internacionalizadas com atuação no mercado brasileiro, como beAnalytic, JoinData, BRQ, Toccato, Nordica, Dataside, Semantix AI, Leega, etc. Por outro lado, identifica-se um crescente número de players de origem nacional, tais como TOTVS, Stefanini, 7COMm, etc.

Estudo do Movimento Brasil Digital e PwC (2022) revela um cenário relativamente pequeno, mas em rápida expansão, de empresas provendo serviços baseados em DLT como a blockchain, com destaque para iniciativas no campo do varejo e fintechs. Alguns exemplos: a Magazine Luiza iniciou as transações de criptomoedas em seu aplicativo, com a compra e venda de Ethereum, Bitcoin e USDC. A Mercado Bitcoin, protagonista em tokenização, oferecendo a comercialização de criptomoedas. A Monnos, oferece uma série de serviços para empresas, o chamado *Blockchain as a Service*. Dentre eles o *Web 3 as a service*, onde efetua a tokenização de programas de fidelidade para o varejo. A Foxbit, atua no campo da tokenização, com serviços como a Foxbit Exchange, Foxbit Pro, Foxbit Pay e Foxbit Invest.

Cabe uma perspectiva dos atores produtores de dados e também usuários de dados e serviços baseados em dados. Conforme esquema acima, a grande maioria dos indivíduos e um percentual crescente das empresas produzem constantemente dados, por intermédio do uso dos mais diversos serviços e softwares e no escopo das diversas funções operacionais e gerenciais das empresas. E, conforme estudos citados acima, as empresas respondem pelo maior percentual

do consumo de serviços baseados em dados. Dada a crescente pervasividade destes papéis de produção e consumo de dados e serviços, não cabe destacar atores no escopo dos indivíduos e empresas.

Os governos nas três esferas possuem importante papel enquanto "produtores" de dados. Estes mobilizam e gerem significativas bases de dados relacionadas às políticas públicas sob sua responsabilidade, com destaque para dados críticos dos cidadãos. O Catálogo de Base de Dados (CBD) oferece um panorama das bases de dados custodiadas pela administração pública federal. Destacam-se o Cadastro Base do Cidadão, as diversas bases agregadas no DataSus na área da saúde, o Cad-único relacionados às políticas sociais, o Cadastro Ambiental Rural, as bases do Sistema Financeiro Nacional e da Receita Federal, entre inúmeras outras. Os órgãos governamentais nas três esferas também possuem importante papel enquanto consumidores de diversos serviços baseados em dados, desde o armazenamento e processamento em datacenters ou por intermédio de serviços de computação em nuvem, até serviços de inteligência artificial, conforme experiências discutidas ao longo deste relatório.

Em termos da infraestrutura para armazenamento e processamento dos dados, destaca-se o cenário brasileiro de datacenters. O tamanho do mercado brasileiro de data centers deverá crescer de US$ 2,10 bilhões em 2023 para US$ 3,03 bilhões até 2028. De acordo com estudo da Mordor Intelligence (2023), existem mais de 120 data centers no país. Esse estudo também revela um mercado muito concentrado. A Ascenty (Digital Realty Trust Inc.) responde por cerca de 35,1% do mercado. A Odata (Patria Investments Ltd) ocupa 14,2% do mercado, a Equinix Inc. 11,4%, a Scala Data Centers 11,4%, a EdgeUno Inc. 4,8%, a Quântico Data Center 3,8%, a Lumen Technologies Inc. 2,7%, a Terremark Inc. (IBM) 2,7%, e a HostDime Global Corp. 2,1%. Além destes datacenters comerciais, observa-se também uma infraestrutura importante de datacenters proprietários de bancos comerciais (Itaú, Bradesco, Banco do Brasil, etc.), empresas de telecomunicações (Vivo, Claro, Oi, etc.), B3, Petrobrás, entre outros.

O mercado de data centers está em processo de rápida ampliação e consolidação nas mãos de grandes players internacionais, como exemplifica a aquisição da ODATA, uma das maiores empresas de Data Centers da América Latina, pela Aligned Data Centers, uma gigante estadunidense do setor e a participação acionária da líder global Digital Reality na Ascenty. Contudo, este segmento também oferece espaço para players de menor dimensão, como é o caso da Scala Data Centers e da Quântico Data Center, citadas acima.

De forma complementar, destaca-se o importante papel de datacenters de organizações vinculadas ao poder público, tais como centros de dados do Banco Central do Brasil, Serpro, Dataprev, Telebrás, Fiocruz[24], Petrobrás, etc.

Grande parte do tráfego atual da internet é facilitado por infraestruturas de datacenters de borda (*edge datacenters*) para diminuir a latência e a sobrecarga de servidores[25]. Nesse escopo, abre-

[24] https://portal.fiocruz.br/noticia/fiocruz-inaugura-1o-datacenter-de-dados-administrativos-e-saude-do-brasil

[25] Um data center de borda é um pequeno data center localizado próximo à borda de uma rede. Fornece o mesmo dispositivo encontrado nos centros de dados tradicionais, mas abrange uma área menor, mais próxima dos usuários finais e dos dispositivos. Estes podem fornecer conteúdo em cache e recursos de computação em nuvem a esses dispositivos.

se espaço para players de menor escala oferecerem serviços de CDN (*content distribution network*). Destaca-se, a iniciativa mobilizada pelo nic.br de OpenCDN, uma iniciativa de compartilhamento de infraestrutura que faculta a CDNs instalarem seus servidores de cache em datacenters em diferentes regiões do Brasil, ligados aos Pontos de Troca de Tráfego de Internet locais do IX.br. Os provedores locais de acesso à internet podem estabelecer um acordo de troca de tráfego bilateral com o OpenCDN, de forma a acessar o conteúdo das CDNs participantes.

De forma articulada aos serviços de datacenters diretamente, destacam-se os serviços de oferta de serviços de hospedagem de sites e datacenters virtuais ou hospedagem em nuvem, um serviço de intermediação entre demandantes de espaço de hospedagem e capacidade de processamento e os provedores de serviços de datacenters. Também neste cenário se destacam os grandes players internacionais, muitos dos quais atuam no mercado brasileiro, com infraestruturas físicas de armazenamento e processamento no país. Dentre os principais players atuantes no mercado nacional, destacam-se empresas de origem internacional, tais como Amazon AWS (57% do mercado brasileiro), Microsoft Azure (28%)[26], Google Cloud, IBM Cloud, Hostinger, Cloudways, Digital Ocean, SiteGround, mas também empresas nacionais, como KingHost, Locaweb, UOL Host, Arquivar, Brasil Cloud e Embratel Primesys. No escopo de organização vinculadas ao governo, destacam-se os serviços de computação em nuvem oferecidos pelo DataPrev para a administração pública (GovCloud), o Serpro MultiCloud e a Telebrás, que projeta se consolidar como principal provedor de serviços de nuvem para o poder público.

Enfoquemos, agora, o Subsistema de Políticas e Representação.

O **Núcleo de Informação e Coordenação do Ponto BR - NIC.br** foi criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br, que é o responsável por coordenar e integrar as iniciativas e serviços da Internet no País. No âmbito do NIC estão:

- Registro.br - Registro de domínios ".br"
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidente de Segurança no Brasil
- Cetic.br - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
- Ceptro.br - Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações
- Ceweb.br - Centro de Estudos sobre Tecnologias Web
- IX.br - Brasil Internet Exchange (PTT.br)

O **Comitê Gestor da Internet no Brasil (CGI)** tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (Internet Protocol) e administração pertinente ao Domínio de Primeiro Nível ".br". Também promove estudos e recomenda procedimentos para a segurança da Internet e propõe programas de pesquisa e

[26] https://www.computerweekly.com/br/reportagen/O-mercado-de-nuvem-cresce-e-se-consolida-no-Brasil ; https://kinsta.com/pt/blog/cloud-market-share/

desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no uso da Internet.

A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia federal de natureza especial vinculada ao Ministério da Justiça, com o objetivo de fiscalizar o cumprimento da LGPD. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) é o órgão consultivo da ANDP.

O **Comitê de Governança Digital da Presidência da República (CGD/PR)**, instituído em 2019, tem por finalidade aprimorar os serviços relacionados à tecnologia da informação e comunicação desenvolvidos na Presidência da República, propondo planos políticas, normas e diretrizes que assegurem o alinhamento destes serviços às necessidades institucionais.

O **Comitê Central de Governança de Dados (CCGD)**, criado em 2019, tem como atribuição deliberar, sobre as orientações e as diretrizes para a categorização de compartilhamento amplo, restrito e específico de dados por órgãos públicos e é responsável por decidir questões sobre integridade, qualidade e consistência dos dados do Cadastro Base do Cidadão (CBC). Além disso, decide quais novos dados serão incluídos no CBC, qual é a prevalência entre eles e a inclusão de novas bases.

O **Serviço de Informação ao Cidadão (SIC)** é a unidade responsável por atender os pedidos de acesso à informação, com base na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

O **Comitê Interministerial para a Transformação Digital (CITDigital)** foi criado pelo Decreto nº 9.319, de 21 de março de 2018.

No âmbito da **segurança cibernética**, identifica-se um complexo arcabouço de organizações. O **Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br)** foi criado no âmbito do Programa de Privacidade e Segurança da Informação (PPSI) e caracteriza-se como uma unidade de coordenação operacional das equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos e das entidades do Sistema de Administração de Recursos de Tecnologia da Informação (SISP). A Rede Federal de Gestão de Incidentes Cibernéticos (REGIC), instituída pelo decreto nº 10.748, de 16 de julho de 2021, tendo como finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos. Atualmente, o Brasil possui oito tipos de centros de tratamento e resposta aos incidentes cibernéticos (CSIRT, de *Computer Security Incident Response Team*), de acordo com sua atuação:

- Centros de Responsabilidade Nacional - CERT.br e CTIR Gov[27];
- Centros de Coordenação Internacional - CERT/Coordination Center, FedCirc e FIRST;

[27] O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br é o responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à internet no País, mais voltado às redes comerciais e de instituições privadas. Com atribuição similar, porém voltado às redes governamentais, existe o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov.

- CSIRTs de Infraestruturas Críticas - Energia - CSIRTCemig - Financeiro - CSIRTs do BB, da Caixa, do BASA, do BNB, do BRB e do BANESE - Telecom - CTIR/DATAPREV, GRA/SERPRO e CSIRT PRODESP;
- CSIRTs de Provedores - CSIRT Locaweb e CSIRT HP;
- CSIRTs Corporativos - CERT-RS,;
- CSIRTs Acadêmicos - CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, SEGTIC UFRJ, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS/UFRN e TRI/UFRGS;
- CSIRTs do Poder Público - Executivo - CTIR Gov, Legislativo - GRIS-CD e Judiciário - GATI, CLRI e TRF-3; e
- CSIRTs Militares - Marinha - CTIM, Exército - CCTIR/EB e Aeronáutica - CTIR.FAB.

No que se refere a Ministérios e órgãos vinculados, destaca-se o papel de:

- Ministério de Ciência, Tecnologia e Inovação (MCTI) - mobilizador de diversos políticas e instrumentos relacionados à digitalização da economia
- Ministério das Comunicações (MC) - políticas voltadas para a área de telecomunicações e infraestrutura da internet
- Ministério da Gestão e da Inovação em Serviços Públicos (MGI) – responsável pela estratégia de governo digital
- Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC) - mobilizador de diversos políticas e instrumentos relacionados à digitalização da economia;
- Ministério da Justiça;
- Casa Civil;
- Secretaria de Comunicação Social (Secom);
- Gabinete de Segurança Institucional;
- Agência Nacional de Telecomunicações (ANATEL)
- Associação Brasileira de Pesquisa e Inovação Industrial (EMBRAPII)
- Agência Brasileira de Desenvolvimento Industrial (ABDI)
- Banco Nacional do Desenvolvimento Econômico e Social (BNDES)

4 Conceituação e Mensuração da Economia de Dados no Brasil

4.1 Conceituações e sistemas de mensuração de economia de dados pelas principais instituições produtoras de estatísticas

O Instituto Brasileiro de Geografia e Estatística (IBGE) foi criado em 1934 e constitui o órgão oficial de estatísticas ligadas às geociências e estatísticas sociais, demográficas e econômicas. Dentre suas funções destaca-se a "coordenação dos sistemas estatístico e cartográfico nacionais". Sua organização de estatísticas referentes às Contas Nacionais, o Censo demográfico, as pesquisas estruturais e temáticas, entre outras, oferecem um conjunto fundamental de informações para a orientação, acompanhamento e avaliação de políticas públicas no país.

Tendo em vista a importância fundamental do órgão e seu papel formal como órgão produtor de estatísticas econômicas, a RedeSist organizou em 05/10/2023 um webinário, tendo como palestrantes convidados os seguintes representantes do IBGE: Alessandro Orlando de Maia Pinheiro; Aline Visconti Rodrigues; Flávio Peixoto. Foram também realizadas entrevistas e reuniões de trabalho com esses e outros representantes do IBGE e do IPEA e a equipe de pesquisa da RedeSist.

Depreende-se das apresentações dos especialistas do IBGE que o órgão ainda não adota uma conceituação de Economia de Dados e que ainda não foram mobilizados esforços para a sua mensuração direta. Contudo, aproximações iniciais se dão a partir do enfoque da economia de dados no escopo mais amplo da Economia Digital. A mensuração da economia digital pode se dar pela ótica da oferta, considerando os diversos subsetores de atividade econômica, adotando como critério de recorte delimitações propostas por organismos internacionais. A este agregado alternativo podem ser associados indicadores relacionados às pesquisas estruturais, tais como valor adicionado, produtividade, média de salários, etc. Adicionalmente, vislumbra-se a possibilidade de aferição da importância de ocupações relacionadas ao tratamento de dados nos diversos setores da economia, considerando ocupações como "cientista de dados" e afins.

A mensuração da Economia Digital também pode se dar pela ótica da demanda, enfocando o uso de produtos digitais, bens, serviços e tecnologias. Este uso pode ser mensurado tanto no âmbito dos domicílios quanto no âmbito das empresas. Destaca-se o esforço em 2023, que se deu no escopo da pesquisa Pintec Semestral, que enfocou o uso de tecnologias digitais avançadas, teletrabalho e cibersegurança em empresas industriais com 100 ou mais pessoas ocupadas[28]. A pesquisa buscou identificar o emprego das seguintes tecnologias digitais avançadas: (i) análise de big data; (ii) computação em nuvem; (iii) inteligência artificial; (iv) internet das coisas; (v) manufatura aditiva; e (vi) robótica. Foi contemplado seu emprego nas seguintes áreas das empresas: (i) desenvolvimento de projetos de produtos, processos e serviços; (ii) produção; (iii) logística; (iv) administração; e (v) comercialização (IBGE, 2023).

[28] https://www.ibge.gov.br/estatisticas/multidominio/ciencia-tecnologia-e-inovacao/35867-pesquisa-de-inovacao-semestral.html?edicao=37966&t=destaques

Uma perspectiva complementar contemplada em pesquisas do órgão diz respeito à "economia da internet". Articulando dados dos registros administrativos do Cempro com dados sobre os registros de sites do NIC.br, uma pesquisa recente do órgão permitiu qualificar o nível de presença online das empresas, a partir de características e grau de complexidade de informações e serviços oferecidos nos sites das empresas[29]. Destacam-se as categorias resultantes nas quais parcela relevante ou principal da receita da empresa se dá através da internet: desde empresas com atuação relevante em e-commerce, empresas que oferecem serviços online, até empresas que oferecem serviços como *webdesign, hosting*, etc., cuja receita é gerada pela internet.

Tendo em vista as perspectivas de mensuração da economia digital e da economia de dados a partir das contas nacionais, com a construção de contas satélite, não se identificaram inciativas por parte do IBGE até o momento em que foi finalizado essa nota técnica.

Embora não figure como órgão produtor de estatísticas oficiais, cabe destaque ao Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br), do NIC.br, enquanto responsável pela realização sistemática de pesquisas sobre o uso de Tecnologias de Informação e Comunicação em diferentes âmbitos da sociedade brasileira. A pesquisas TIC-Empresa, por exemplo, é realizada desde 2005 e explora diferentes aspectos do acesso às TICs o uso de tecnologias básica como os computadores, a internet e softwares, o uso de serviços de governo eletrônico, as habilidades para uso destas tecnologias, entre outros aspectos. Pesquisas enfocadas em setores específicos, como a TIC-Saúde e a TIC-Educação, além dos aspectos gerais de emprego de TICs, exploram as aplicações específicas destas tecnologias nestes setores de atuação. No primeiro caso, destaca-se o emprego destas tecnologias em serviços de telessaúde. No segundo caso, destaca-se a avaliação do seu emprego nas propostas pedagógicas e, sobretudo, a existência de orientação para o uso crítico, seguro e responsável de TICs, elemento de central importância em uma perspectiva de soberania e autodeterminação individual.

A pesquisa TIC-Domicílios também é realizada desde 2005 e explora aspectos relacionados ao acesso às TIC, uso de tecnologias como computador, internet e celular, além do uso de serviços online como comércio eletrônico e governo eletrônico. Desde 2012, a pesquisa Kids-*Online* complementa esta perspectiva do setor institucional domicílios, explorando oportunidades e riscos relacionados à participação *on-line* da população de 9 a 17 anos.

A pesquisa TIC – Governo Eletrônico investiga a incorporação das TIC nos órgãos públicos, tendo em vista a ampliação do acesso aos serviços públicos, da transparência dos governos, da participação do cidadão. A edição de 2021 também explorou aspectos relacionados à privacidade e proteção de dados pessoais, tendo em vista a adequação dos órgãos à Lei Geral de Proteção de Dados Pessoais (LGPD).

Ademais, cabe destaque também à pesquisa TIC Provedores, que busca prover um mapeamento do setor de provimento de serviço de acesso à Internet no Brasil, explorando a diversidade e qualidade dos serviços oferecidos, a atuação no mercado e a adoção de tecnologias, com destaque para protocolo de internet e segurança de dados.

[29] https://repositorio.cepal.org/bitstream/handle/11362/48908/1/S2300394_es.pdf

Em suma, tanto as pesquisas mencionadas do IBGE, quanto as pesquisas conduzidas pelo CETIC.br não apresentam uma conceituação explícita de "economia de Dados", se alinhado a uma perspectiva ampla de Economia Digital e digitalização da economia. As pesquisas, em seu conjunto, se apresentam bastante abrangentes em termos de cobertura dos diversos setores institucionais utilizadores de tecnologias digitais. Contudo, sob o ponto de vista da cadeia de valor da economia de dados propriamente dita, os estudos não enfocam e não detalham atores e atividades relacionadas à armazenagem e custódia de dados, captura e processamento, análise de dados e produção de conhecimento, e contemplam parcialmente o consumo final de bens e serviços por intermédio do uso de tecnologias e serviços habilitados a partir de dados, tais como big data e inteligência artificial.

Contudo, discursos da presidência do IBGE, iniciada em 2023, e iniciativas que começam a se estruturar apontam para um entendimento mais consolidado da economia de dados e para a perspectiva multidimensional de soberania digital e de dados. Em primeiro lugar, destaca-se a intenção explicitada pelo presidente da instituição de atuar junto a diferentes instâncias da administração federal para avançar na constituição de um *data lake* (agregação e estruturação de bases de dados), formado a partir das mais diversas bases de dados constituídas e geridas por órgãos vinculados ao governo. Tal agregação de bases de dados e seu acesso pelo IBGE facultaria o órgão a construir estatísticas mais abrangentes e estruturadas, auxiliando os diversos órgãos na concepção, construção, acompanhamento e avaliação de políticas públicas.

Em segundo lugar, destaca-se o acordo de cooperação técnica recém celebrado entre o IBGE e a Universidade Federal de Goiás (UFG) e a Universidade Estadual de Campinas (Unicamp) para o desenvolvimento do projeto inteligência artificial aplicada às políticas públicas. Objetiva-se desenvolver ferramentas conversacionais, aos moldes do ChatGPT, a ser utilizado por gestores públicos, para auxiliar na elaboração de diagnósticos e de programas com uso de Inteligência Artificial. Depreende-se da comunicação do presidente da instituição, que o projeto se alinha com uma perspectiva de soberania relacionada à "promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços", na medida em que visa-se mobilizar competências nacionais no desenvolvimento de ferramentas de análise e processamento de dados relacionados às políticas públicas[30].

4.2 Perspectivas do Marco Legal

4.2.1 A Construção de um Marco Legal

Como ponto de partida, cabe explicitar os dispositivos presentes na Constituição Federal de 1988 que conceituam uma noção de soberania. O art. 1 estabelece como primeiro fundamento o princípio da soberania (política) e esta se articula diretamente com a soberania econômica, primeiro princípio da Ordem Econômica Constitucional, conforme art. 170. Ao afirmar que a ordem econômica tem por finalidade "assegurar a todos existência digna, conforme os ditames da justiça social" (art. 170) e que compete ao Estado "as funções de fiscalização, incentivo e

[30] https://www.convergenciadigital.com.br/Inovacao/IBGE-vai-usar-inteligencia-artificial-em-dados-para-estados-e-municipios-64858.html

planejamento" (art. 174), a Constituição Federal insere a "soberania econômica" em um contexto mais amplo de uma estratégia de desenvolvimento. Conforme determina o art. 2019 "o mercado interno integra o patrimônio nacional e será incentivado de modo a viabilizar o desenvolvimento cultural e socioeconômico, o bem-estar da população e a autonomia tecnológica do País".

Coloca-se, portanto, a necessidade de políticas públicas orquestradas com o fim de superação da condição de subdesenvolvimento, que tem no atraso e dependência científico e tecnológico determinantes centrais. É neste sentido que o art. 218 determina que o Estado "promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação". E o §2º deste artigo reforça o entendimento de soberania econômica e política ao frisar que a "pesquisa tecnológica voltar-se-á preponderantemente para a solução dos problemas brasileiros e para o desenvolvimento do sistema produtivo nacional e regional".

Portanto, a Ordem Econômica Constitucional, centrada na afirmação da soberania nacional e na identificação do mercado interno como um patrimônio a ser estimulado com o fim de promoção do desenvolvimento com autonomia tecnológica, atribui um papel central ao Estado no atual contexto de transformação digital. Cabe ao Estado a mobilização de instrumentos de fiscalização, incentivo e planejamento, com fim de desenvolvimento e domínio de tecnologias críticas da economia digital, de forma a reduzir a dependência de tecnologias estrangeiras e garantir a soberania nacional em sentido amplo.

Tomando como referência as dimensões de objetivos de promoção da soberania discutidas anteriormente, fica evidente que a Constituição Federal contempla, de forma articulada, todas as quatro dimensões. Uma perspectiva ampla de soberania nacional se articula com sua manifestação na esfera econômica e o papel do mercado interno e do desenvolvimento científico e tecnológico. Os dispositivos do art. 5, que versa sobre direitos e fundamentais, subordina a ordem política e econômica à garantia de autodeterminação individual e à proteção da identidade e diversidade sociocultural do país.

É neste contexto, e alinhado aos desafios trazidos pelo progresso das tecnologias digitais, que se mobiliza o marco legal que regulamenta a internet que disciplinam seu funcionamento, como o Marco Civil da Internet e a Lei geral de Proteção de Dados Pessoais.

4.2.2 A Institucionalização da Internet no País

A Norma nº 004/1995[31] do Ministério das Comunicações definiu o "Serviço de Conexão à Internet" como um "Serviço de Valor Adicionado" e a Portaria Interministerial nº 14/1995 criou o Comitê Gestor da Internet, estabelecendo-se as bases para a exploração comercial dos serviços de acesso à internet por parte da iniciativa privada. Conforme coloca Paz Filho (2013), o Estado optou por uma "regulação minimalista e por camadas", limitando ao máximo a interferência do poder público na prestação deste serviço.

[31] Aprovada pela Portaria nº 148, de 31 de maio de 1995, do Ministério da Ciência e Tecnologia.

A Lei Geral de Telecomunicações (Lei nº 9.472/1997) estabeleceu a Agência Nacional de Telecomunicações (Anatel) como reguladora da infraestrutura física e dos serviços de telecomunicações necessários para a provisão do acesso à internet, com impacto direto sobre a atual adoção e difusão de tecnologias críticas, como fibra ótica, 5G e internet das coisas. Por outro lado, a ANATEL não possui ingerência sobre a comada de conteúdo da internet propriamente dita.

O Comitê Gestor da Internet (CGIbr) tem sua organização atual determinada pelo decreto nº 4.829/2003, que estabelece a participação de 21 representantes dos setores público e privado (9 do setor público, 4 do setor empresarial, 4 do terceiro setor, 3 da comunidade científica e tecnológica e um representante de notório saber em assuntos de Internet). Dentre as suas atribuições, destacam-se: "I - estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil"; "III - propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular a sua disseminação em todo o território nacional"; " IV - promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade"; "V - articular as ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à Internet". Atribuições como as de execução do registro de Nomes de Domínio, a alocação de Endereço IP (Internet Protocol) e a administração relativa ao Domínio de Primeiro Nível foram atribuídas ao Núcleo de Informação e Coordenação do Ponto Br (NIC.br).

4.2.3 O Marco Civil da Internet

O Marco Civil da Internet, instituído pela lei nº 12.965, de 23 de abril de 2014, contribui para regulamentar importantes aspectos relacionados às dimensões do conteúdo e dos serviços providos por plataformas. O documento legal não apresenta uma definição de economia digital ou de economia de dados. Contudo, uma análise de seu conteúdo permite identificar as dimensões priorizadas.

Enquanto "marco civil", a lei atribui forte peso a imperativos de soberania relacionados à promoção de autonomia dos usuários e de autodeterminação individual.

Destaca-se a garantia de direitos fundamentais a partir dos preceitos de liberdade de expressão (art. 2), de privacidade e de neutralidade da rede (art. 3). Na mesma linha, o art. 7 reconhece o acesso à internet como "essencial ao exercício da cidadania" e garante a "inviolabilidade da intimidade e da vida privada" e a "inviolabilidade e sigilo do fluxo de suas comunicações".

O uso indiscriminado de dados gerados pelos usuários durante seu ato de uso de aplicações de internet é limitado por diversos dispositivos. O item VII do art. 7 determina o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei". E o item VIII exige que sejam providas "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação;

e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet". O item X, por sua vez, garante ao usuário o direito de "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes".

A isenção de responsabilidade das plataformas digitais pelo conteúdo gerado pelos usuários (art. 18), adotando padrão dos Estados Unidos, contribui para reforçar a liberdade de expressão e para coibir práticas de censura. Contudo, aponta-se que a "ausência de obrigações de transparência e *accountability*" neste documento legal contribuiu para a proliferação de desinformação e de atividade maliciosa nas plataformas digitais, sem que as empresas tenham tido a obrigação de remoção de conteúdo.

Dentre as diretrizes para a atuação do Estado, destaca-se o item I do art.24 que ratifica o modelo de gestão adotado com o Comitê Gestor da Internet (CGIbr), ao preconizar "mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica".

Contudo, talvez a diretriz mais importante - em termos da promoção da soberania relativa à promoção de autonomia dos usuários e de autodeterminação individual - possa ser encontrada no art. 26: "O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico". Tal preceito se alinha a diretrizes perseguidas em diversos países de promoção de educação e conscientização crítica para um uso "soberano" da internet, associado, por exemplo, ou preceito da política alemã de "consciência de dados".

As demais dimensões de objetivos relativos à soberania digital e de dados não encontram repercussão relevante no Marco Civil da Internet. As referências são muito pontuais.

Este é o caso, por exemplo, com relação à promoção da segurança nacional e do estado de direito. O dever de guarda e disponibilização dos registros de conexão e de acesso dos usuários (art. 10 e 11) se alinha com tal perspectiva, ao garantir a persecução cível e criminal e o *enforcement* legal na internet. De resto, um alinhamento com um objetivo de promoção da segurança nacional é verificado, de forma pontual e pouco específica, na diretriz para atuação do Estado nº VII (art.24) ao indicar a "otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País".

Também virtualmente ausente no documento legal é a preocupação com diretrizes de soberania alinhados à promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços. A lei faz menções vagas a "livre iniciativa" (art.2), "liberdade dos modelos de negócio" (art.3), "inovação e fomento à ampla difusão de novas tecnologias e modelos de uso", "adoção a padrões tecnológicos abertos" (art.4) e "adoção preferencial de tecnologias, padrões e formatos abertos e livres" (art. 24). A única menção pontual e indireta à promoção de capacidades técnicas e competitivas nacionais está na diretriz de atuação do Estado, já mencionada acima, que versa sobre a implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, na medida em que se associa tal promoção de

atividade no país à promoção da "qualidade técnica, a inovação e a difusão das aplicações de internet".

4.2.4 Lei Geral de Proteção de Dados Pessoais

A LGPD (Lei nº 13.709/2018) possui inspiração na legislação europeia (*General Data Protection Regulation - GDPR*). Ela provê um arcabouço legal amplo para a proteção de dados digitais ou não e detalha e regulamenta direitos, deveres e procedimentos em complementação ao Marco Civil da Internet. Embora não forneça nenhuma conceituação de economia de dados, a lei contempla a diversidade de atividades usualmente presentes em definições. Assim, o item X do art. 5 define o tratamento de dados como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Tendo em vista a perspectiva ampla do Sistema Produtivo e Inovativo na Economia de Dados, cabe destacar a diversidade de atores relevantes previstas pela lei. Ao se referir a "controlador", "operador" e "encarregado", a lei sistematiza os principais papeis que podem ser exercidos por diversos atores, tais como provedores de serviços online e plataformas digitais no tratamento de dados pessoais. Ao fazer referência às finalidades explicitamente informadas de uso dos dados pessoais, a lei vislumbra o papel da diversidade de atores de diferentes segmentos produtivos no consumo intermediário de dados e serviços relacionados, bem como as possíveis modalidades de consumo final. A lei também prevê o papel dos "órgãos de pesquisa", mas sob o prisma de seu papel enquanto geradores e utilizadores de dados em suas atividades de pesquisa diversas e não enquanto atores críticos para o desenvolvimento de tecnologias adequadas à geração, tratamento e aplicação de dados, alinhados a preceitos de soberania de dados. Tampouco há referência a atores industriais produtores de hardwares e softwares embarcados, não se reconhecendo a potencial interface entre padrões técnicos empregados em produtos e serviços e a própria capacidade de aceso à informação e de fazer cumprir o disposto na lei em termos de proteção de dados. Por fim, a lei traz um papel destacado para o poder público, sobretudo por intermédio das atribuições da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Alinhado ao seu próprio propósito, a LGPD possui foco central em aspectos que podemos relacionar à dimensão de soberania relativa a promoção de "autonomia dos usuários e de autodeterminação individual". Neste sentido, os fundamentos que regem a lei destacam "privacidade", "autodeterminação", "liberdade de expressão", intimidade, honra e imagem", dignidade e exercício da cidadania" (art. 2). Na mesma linha, os princípios e limites à atividade de tratamento de dados (art.6) e o conjunto de direitos relativos ao consentimento (art. 7) para uso de dados pessoais ou sua revogação (art. 8), a possibilidade de exigência de acesso, correção e eliminação de dados (art. 18) reforçam este aspecto de soberania individual e autodeterminação.

Com relação à soberania em termos "segurança nacional e defesa do estado de direito" a lei traz alguns provimentos. Em primeiro lugar, o art. 4 determina que as limitações impostas pela lei não se aplicam no escopo da atuação do Estado na provisão de "segurança pública"; "defesa nacional" e "segurança do Estado"; e o § 4º determina que os bancos de dados relacionados a tais funções não poderão ser tratados por pessoa de direito privado. Desta forma, é assegurado o tratamento direto por órgão vinculado ao Estado e em território nacional de dados críticos à segurança nacional.

Em segundo lugar, o art. 33 estabelece um conjunto de limitações e condicionantes para a transferência internacional de dados pessoais. Cabe destaque para o item I que limita tal transferência a países ou organismos internacionais que proporcionem grau de proteção de dados pessoais alinhados à LGPD. Em tese, tal disposto excluiria serviços de internet e de processamento de dados situados no EEUU, cuja legislação não apresenta tal alinhamento previsto com a legislação nacional. Por outro lado, o item II constitui um afrouxamento excessivo, tornando o item I potencialmente sem efeito prático, na medida em que baste ao controlador no exterior apresentar cláusulas contratuais que garantam os direitos previstos na LGPD, mesmo sem que exista capacidade de *enforcement* internacional para o cumprimento de tais cláusulas. Ademais, embora apresente relevante distinção entre "dado pessoal" e "dado pessoal sensível", a lei não apresenta nenhuma distinção quanto ao tipo, natureza ou localização do controlador ou operador que tratarão estes dois tipos de dados, não reconhecendo uma importância diferenciada da proteção do segundo conjunto.

Em terceiro lugar, a lei apresenta apenas uma referência genérica e pouco específica à questão da proteção dos dados, ao determinar no art. 46 que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Não há nenhuma ponderação acerca de dados pessoais críticos associados à provisão de serviços públicos e adoção de infraestruturas e padrões técnicos unificados e públicos para a proteção destes dados. Tampouco há, conforme apontado acima, nenhuma consideração acerca da interface entre padrões técnicos adotados nos serviços de conexão e nos serviços digitais e a capacidade de aceso à informação e de fazer cumprir o disposto na lei em termos de proteção de dados. Conforme argumenta Peck (2023)[32], na ausência de uma regulamentação do artigo 46 que detalhe padrões técnicos mínimos de segurança de dados, "todos os dias ocorrem licitações cujos editais não conseguem especificar adequadamente as exigências de requisitos de proteção e segurança de dados alinhados à LGPD e à uma perspectiva de soberania digital".

No que diz respeito a diretrizes de soberania relacionadas à "promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços", não se observa virtualmente nenhuma menção explícita ou implícita na lei. Mesmo que a lei destaque como um dos seus fundamentos, no art. 2 o "desenvolvimento econômico e tecnológico e a inovação", não há nenhuma referência a um potencial papel de atores econômicos nacionais ou de instituições de pesquisa nacionais no desenvolvimento de tecnologias e padrões técnicos

[32] https://neofeed.com.br/experts/e-preciso-falar-sobre-soberania-digital/

convergentes com os dispositivos da lei. Mesmo que preveja limitações ao tratamento de dados no exterior, como dito, estas limitações possuem pouca relevância prática, não havendo obstáculos para que provedores estrangeiros de pacotes de serviços de dados "capturem" parte substancial do mercado de dados do país, especialmente tendo em visto os imperativos de menor preço impostos pela legislação de compras públicas.

Por fim, cabe destacar que, por tratar exclusivamente de dados pessoais, a LGPD não estende a mesma proteção e disposição à uma diversidade de outros dados, muitos dos quais de suma importância sob o ponto de vista da soberania e segurança nacional. Dados sobre infraestruturas críticas das cidades, dados sobe o sistema financeiro nacional ou dados sobre a operação do sistema elétrico do país (SIN), entre outros, não são protegidos por legislação equivalente, podendo colocar em risco sistemas críticos.

4.2.5 Outras Leis Relacionadas à Governança de Dados e Serviços Relacionados

O Decreto nº 8.777/2016, institui a Política de Dados Abertos do Poder Executivo Federal. De acordo com seu propósito, o decreto enfoca especificamente os dados considerados acessíveis ao público (qualquer dado gerado ou acumulado pelo Governo que não esteja sob sigilo ou sob restrição de acesso nos termos da Lei nº 12.527, de 18 de novembro de 2011), estruturados na forma de dados abertos (dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte). O decreto determina também que cabe à Controladoria-Geral da União, por meio da Infraestrutura Nacional de Dados Abertos – INDA, a gestão da Política de Dados Abertos do Poder Executivo federal.

Dado seu foco, o documento não contempla questões relacionadas à proteção de dados. Contudo, tampouco contempla ponderações a respeito de seu uso ético, o que pode ser de importância central, tendo em vista a utilização destes dados para treinar sistemas de inteligência artificial e mobilizar serviços baseados em IA para auxiliar a construção, gestão e avaliação de políticas públicas.

O Decreto nº 10.046, de 9 de outubro de 2019 dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Para qualificar o grau e condições de compartilhamento de dados, o decreto define três níveis, de acordo com sua confidencialidade:

> I - compartilhamento amplo, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;
>
> II - compartilhamento restrito, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e

> III - compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.

Especialmente importante sob o ponto de vista da soberania de dados é o disposto no artigo sétimo, que determina padrões de segurança para plataformas que sejam utilizadas para o compartilhamento de dados, sobretudo os de compartilhamento restrito e específico:

> Art. 7º As plataformas de interoperabilidade contemplarão os requisitos de sigilo, confidencialidade, gestão, auditabilidade e segurança da informação necessários ao compartilhamento de dados, conforme regras estabelecidas pelo Comitê Central de Governança de Dados.
>
> Parágrafo único. As ferramentas de gestão da plataforma de interoperabilidade incluirão meios para que o gestor de dados tenha conhecimento sobre o controle de acesso e o consumo dos dados.

Por outro lado, o decreto não impõe nenhuma limitação com relação a que tipo de atores podem oferecer serviços de interoperabilidade, não excluindo a possibilidade de dados protegidos por sigilo serem transmitidos por redes que incluam infraestruturas e atores privados e fora do país. Sob este ponto de vista, o decreto não apresenta um alinhamento com objetivos de soberania digital e de dados relacionados à 'soberania nacional'.

O decreto também institui o Comitê Central de Governança de Dados (CCGD), responsável por decidir questões sobre integridade, qualidade e consistência dos dados do Cadastro Base do Cidadão (CBC), além de decidir quais novos dados serão incluídos no CBC, qual é a prevalência entre eles e a inclusão de novas bases.

O Projeto de Lei 21/20 cria o marco legal do desenvolvimento e uso da Inteligência Artificial (I.A.) pelo poder público, por empresas, entidades diversas e pessoas físicas. O texto, em tramitação na Câmara dos Deputados, estabelece princípios, direitos, deveres e instrumentos de governança para a I.A. O PL apresenta amplo alinhamento com diretrizes de soberania digital e de dados relacionados a 'promoção de autonomia dos usuários e de autodeterminação individual'.

Entre outros pontos, a proposta estabelece que o uso da I.A. terá como fundamento o respeito aos direitos humanos e aos valores democráticos, a igualdade, a não discriminação, a pluralidade, a livre iniciativa e a privacidade de dados. Além disso, a I.A. terá como princípio a garantia de transparência sobre o seu uso e funcionamento.

O projeto de lei também propõe que agentes responsáveis pelo desenvolvimento e implantação de serviços de IA terão deveres, como responder, legalmente, pelas decisões tomadas por um sistema de inteligência artificial e assegurar que os dados utilizados respeitam a Lei Geral de Proteção de Dados (LGPD). Ademais, o projeto prevê o estímulo à adoção de IA nos serviços públicos, preferencialmente em formato aberto e livre, além do apoio a pesquisas na área,

capacitação de trabalhadores para se adaptarem à nova realidade tecnológica e criação de mecanismos de governança[33].

Por fim, cabe destacar o Projeto de Lei Complementar nº 234/2023 que propõe a instituição da Lei Geral de Empoderamento de Dados e dispõe sobre o Ecossistema Brasileiro de Monetização de Dados. O projeto apresenta uma proposta detalhada de definição e especificação de diferentes atores e função da economia de dados, provendo uma perspectiva ampla de o que aqui se define como a cadeia de valor no cerne do sistema produtivo e inovativo da economia de dados:

> Art. 11. São participantes do Ecossistema Brasileiro de Monetização de Dados:
>
> I - no caso do compartilhamento de dados de que tratam os incisos I a III do art. 8º, quaisquer empresas que ofertem produtos ou serviços por meio da Rede Mundial de Computadores e coletem, processem ou distribuam dados pessoais de titulares, comercializem ou monetizem dados, individualmente ou mediante agrupamento, ainda que anonimizados, pseudonomizados ou despersonalizados, por meio de: a) plataformas eletrônicas online; b) portais e sítios; c) aplicações de internet para computador pessoal ou aparelhos de telefonia móvel ou quaisquer outros aparelhos que permitam o acesso à internet; d) programas de computador; e) dispositivos de qualquer espécie, conectados à rede mundial de computadores, que gerem dados relacionados ao seu usuário, inclusive em âmbito doméstico, passíveis de serem coletados, processados ou distribuídos.
>
> II - os marketplaces e portais ou aplicações de internet para comércio eletrônico;
>
> III - no caso do compartilhamento de dados de que trata o art. 8º, inciso IV, as entidades sujeitas à regulação e fiscalização do Banco Central do Brasil, nos termos de norma específica editada pelo Conselho Monetário Nacional e o Banco Central do Brasil, no exercício de suas competências.

A proposta de definição do "Ecossistema Brasileiro de Monetização de Dados", no artigo quarto, apresenta uma perspectiva ampla de soberania relacionada a 'promoção de autonomia dos usuários e de autodeterminação individual', nos moldes de legislações que estão sendo gestadas em diversos países europeus e na união europeia:

> Art. 4º. O Ecossistema Brasileiro de Monetização de Dados é o ecossistema de dados por meio do qual as pessoas físicas e jurídicas residentes ou com sede no território nacional atuam na produção, coleta, armazenamento, custódia, distribuição, compartilhamento e processamento de dados, com

[33] https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-no-brasil/

> vistas a objetivos comuns, definidos livremente entre as partes, nos termos de contrato regido pelo disposto nesta Lei Complementar e pelo Código Civil Brasileiro e normas legais ou regulamentares específicas, assegurada a participação do titular dos dados nos resultados econômicos decorrentes da sua distribuição, agrupamento, compartilhamento, processamento ou disseminação pelas instituições detentoras de contas de dados, transmissoras de dados, receptoras de dados ou iniciadoras de transação de dados.

O empoderamento dos indivíduos é reforçado pela proposta dos artigos nono e décimo:

> Art. 9º. As instituições referidas no art. 2º deverão notificar os titulares de dados de que as informações de que os dados e informações abrangidos pelo Ecossistema Brasileiro de Monetização de Dados podem ser compartilhadas e que os titulares têm o direito de autoexclusão da permissão de compartilhamento de seus dados e informações pessoais.
>
> Art. 10. O titular tem o direito de, a qualquer tempo, dirigir uma instituição referida no art. 2º manifestação para não compartilhar os dados ou informações pessoais ou relacionadas a transações de qualquer natureza de que participe.

Cabe uma apreciação do projeto de lei complementar à luz das quatro dimensões de soberania digital e de dados elencadas como referência para este estudo. Embora o projeto de lei complementar constitua importante avanço sob o ponto de vista da promoção de autonomia dos usuários e de autodeterminação individual, o projeto não contempla as demais dimensões de soberania consideradas relevantes. Não há considerações sobre aspectos de 'segurança nacional' e a natureza especialmente crítica de dados relacionados a diversos sistemas e infraestruturas vitais para a sociedade. Embora proponha um conjunto de dispositivos para regulamentar e regular o mercado de dados no país, não se observa nenhuma orientação relacionada à natureza e origem dos atores e tecnologias empregadas, negligenciando uma perspectiva de soberania relacionada à "promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços". Tampouco são contemplados aspectos relacionados à "proteção da identidade e diversidade sociocultural, promovendo a proteção do patrimônio cultural, a diversidade linguística".

BOX 1

Empresas e órgãos públicos podem contratar data centers no exterior?

Para responder a esta pergunta, Oliveira (2017) apresenta uma análise detalhada das leis e dos dispositivos infra legais, cujos principais aspectos são sumarizados a seguir. Como ponto de partida cabe destacar que na época da instituição do Marco Civil da Internet, o então Projeto de Lei 2.126/2011 incorporava a tentativa do governo de vedar amplamente a utilização de data centers no exterior. Conforme redação original do artigo 12:

> Art. 12 O Poder Executivo, por meio de Decreto, poderá obrigar os provedores de conexão e de aplicações de internet previstos no art. 11 que exerçam suas atividades de forma organizada, profissional e com finalidades econômicas a instalarem ou utilizarem estruturas de armazenamento, gerenciamento e disseminação de dados em território nacional, considerando o porte dos provedores, seu faturamento no Brasil e a amplitude da oferta do serviço ao público brasileiro.

Este dispositivo no projeto de lei ia de encontro a episódios recentes, como a decisão do STJ no Inquérito 784-DF determinando que a empresa Google entregasse à Justiça brasileira dados sigilosos de e-mails trocados entre investigados, a qual foi prontamente ignorada pela empresa estadunidense[34]. A efetiva localização em território nacional garantiria que provedores de serviços não pudessem se furtar a observar a legislação e a justiça brasileiras. Também convergia para tal proposta as preocupações com a segurança nacional, em face de denúncias de que agências estadunidenses estariam monitorando órgãos do governo brasileiro. E, certamente, os investimentos em infraestruturas deste tipo no país tenderiam a mobilizar serviços e produtos de diversos segmentos relacionados no país.

Contudo, a proposta de artigo enfrentou resistências no congresso e acabou por ser retirada do projeto de lei. Permaneceu apenas a obrigação de que toda operação de coleta e de guarda de registros prestada a brasileiros deva obedecer a legislação brasileira, mesmo que a empresa esteja situada no exterior:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> §1° O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> §2° O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

E ainda o artigo 24, item VII, apresenta uma diretriz vaga de atuação dos entes da administração pública para estimular o desenvolvimento de datacenters no país: “otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação

[34] https://www.migalhas.com.br/quentes/190244/marco-civil-da-internet-obriga-guarda-de-dados-no-brasil

e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa".

Outro movimento importante alinhado com a soberania de dados se deu com a publicação, pelo Ministério do Planejamento, Orçamento e Gestão, em maio de 2016, do "Manual de Boas Práticas, Orientações e Vedações para Contratação de Serviços de Computação em Nuvem". No Item 8, o documento determina que os órgãos contratantes de serviços de computação em nuvem devam exigir que os dados sejam armazenados em território nacional:

> 8. Os órgãos deverão exigir, por meio de cláusulas contratuais, em conformidade com o disposto na NC 14/IN01/DSIC/GSIPR, que os dados e informações do contratante residam exclusivamente em território nacional, incluindo replicação e cópias de segurança (backups), de modo que o contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem.

A Norma Complementar 14/IN01/DSIC/GSIPR citada foi emitida pelo Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a utilização de computação em nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF) direta e indireta. Contudo, tal norma complementar não impõem a obrigação o armazenamento de dados em infraestrutura fisicamente localizada no país. Ela apenas determina que:

> 5.3. Os órgãos ou entidades da APF devem avaliar quais informações serão hospedadas na nuvem, considerando: (…)
>
> 5.3.5. A localização geográfica onde as informações estarão fisicamente armazenadas.

E para garantir a disponibilidade dos dados, a norma complementar determina que

> 5.2.3. O contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

Portanto, o disposto no manual de boas práticas possui um efeito apenas indicativo e sem força legal, uma vez que a norma complementar a qual se refere não impõe uma localização de dados. E nem poderia impor, pois estaria em desalinho com a legislação, notadamente o Marco Civil da Internet e a LGPD, que não impõem tal limitação, conforme discutido acima.

Cabe destacar também o Acórdão 1.739-24/15-P do Tribunal de Contas da União (TCU), proferido nos autos do Processo 025.994/2014-0, que analisa a utilização do serviço de

computação em nuvem por órgãos governamentais. Destaque para o artigo primeiro que determina:

> Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias. (…)
>
> § 4º O armazenamento e a recuperação de dados a que se refere o caput deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal.

Contudo, no inciso II do §5° é determinado:

> § 5º Ato conjunto dos Ministros de Estado da Defesa, do Planejamento, Orçamento e Gestão e das Comunicações disciplinará o disposto neste artigo e estabelecerá procedimentos, abrangência e prazos de implementação, considerando:
>
> I – as peculiaridades das comunicações dos órgãos e entidades da administração pública federal; e
>
> II – a capacidade dos órgãos e entidades da administração pública federal de ofertar satisfatoriamente as redes e os serviços a que se refere o caput.

Os Ministros de Estado da Defesa, do Planejamento, Orçamento e Gestão e das Comunicações editaram a Portaria Interministerial 141/2014, estabelecendo procedimentos para a contratação de serviço de comunicação de dados. No §3° do artigo 5, é determinado:

> § 3º Nas hipóteses dos §§ 1º e 2º, até o término da fase de planejamento da contratação, o órgão ou entidade contratante deverá consultar a regulamentação do órgão gerenciador ou os órgãos ou entidades fornecedores que prestem serviços compatíveis com o objeto da contratação sobre a disponibilidade para atendimento das especificações técnicas e níveis de serviço do objeto do contrato, conforme o caso.

De forma complementar, o artigo 7° determina:

> Art. 7º Nos casos em que não houver oferta da prestação de serviços por órgãos ou entidades fornecedores, é permitida a contratação de serviços de redes de telecomunicações ou de tecnologia da informação junto a fornecedores privados.
>
> § 1º Para fins desta Portaria, o serviço será considerado não ofertado quando o órgão ou entidade fornecedor:
>
> I – não atender à localidade da prestação do serviço;

> II – não atender aos requisitos técnicos relativos à infraestrutura ou aos serviços, conforme demandado pelo órgão ou entidade contratante, observada a regulamentação estabelecida pelo órgão gerenciador, quando houver;
>
> III – não responder à consulta formal sobre o atendimento dos serviços no prazo de trinta dias; e
>
> IV – não puder enquadrar a demanda do órgão ou entidade contratante nas prioridades de contratação de que trata o art. 4º, inciso I, alínea "a".

Depreende-se que a contratação dos serviços referidos junto a entidades da administração pública federal não é obrigatória se não existir capacidade de provisão dos serviços, nos moldes demandados, por parte das entidades públicas. Neste caso, é facultada a contratação junto a fornecedores privados, não havendo distinção quanto à localização de sua infraestrutura de base.

Neste contexto, a unidade técnica do TCU, realizou avaliação dos serviços de nuvem oferecidos por empresas públicas, sendo identificadas, em 2016, duas prestadoras potenciais: Dataprev e o Serpro. Na época a Dataprev ainda não tinha iniciado a oferta do serviço e, no que se refere ao Serpro, a equipe do TCU considerou que a organização não disporia da capacidade para prover o serviço.

Contudo, conforme detalhado abaixo, os dois órgãos estruturaram seus serviços de computação em nuvem voltados para a administração pública e, em 2023, oferecem serviços estruturados: GovCloud do DataPrev e o Serpro MultiCloud, além de outros órgãos. Neste cenário, a observação do disposto no acórdão do TCU implicaria na priorização da contratação, por parte de organização governamentais, de serviços junto a estes provedores públicos.

Em suma, as leis, destacadamente o Marco Civil da Internet e a LGPD, que se sobrepõem aos dispositivos infra legais, não obrigam a contratação de serviços junto a fornecedores com determinada característica em termos de natureza jurídica ou localização. Mas também não indicam, explicitamente, o contrário, de que organizações públicas e privadas, situadas ou não no país deveriam gozar das mesmas condições quando da concorrência pela prestação de serviços junto a órgãos governamentais. Neste contexto, os dispositivos infra legais citados, em um contexto em que existe, atualmente, ampla capacidade de prestação de serviço por órgãos vinculados ao poder público, deveriam ter poder vinculante, vedando a contratação de serviços de nuvem junto a empresas privadas que não armazenam os dados em datacenters no Brasil.

De forma complementar a esta discussão, cabe destacar a lei nº 14.744 recém aprovada em 30 de novembro de 2023, que determina que os órgãos públicos federais da administração direta e as entidades da administração indireta federal devem, preferencialmente, contratar diretamente a Telebrás para utilização de serviços de comunicação multimídia. Considerando a oportunidade que tal lei consolida e a disponibilidade de infraestrutura de datacenter de alto

desempenho (Tier IV), a Telebrás objetiva se consolidar como principal provedor de serviços de computação em nuvem para a administração pública no país[35].

4.3 Perspectivas das Políticas Governamentais

4.3.1 Estratégia Brasileira para Transformação Digital (E-digital)

A Estratégia Brasileira de Transformação Digital (Brasil, 2018) teve sua primeira versão lançada em 2018, destacando como desafio a ampliação da infraestrutura de telecomunicações para as áreas deficientes de cobertura e para a população de baixa renda. Em termos de infraestrutura, a estratégia destacava a reduzida presença de data centres no país e definia "como estratégico que o Brasil construa mecanismos de atração de centros de dados", tendo em vista que "aumentar o número de centros de dados no País significa conferir maior governança sobre o conteúdo e, consequentemente, maior segurança para os dados de empresas e de cidadãos". O documento também apresentava uma preocupação com "o risco de concentração do poder econômico no mercado de plataforma digitais, o que exige atualização e avaliação por parte das autoridades regulatórias e de antitruste" e destaca a importância do "estímulo ao desenvolvimento de empresas nacionais atuantes nos mercados de plataformas digitais, buscando ampliar a segurança jurídica e a apropriação dos ganhos de exploração desses mercados".

Em dezembro de 2022, foi publicada uma atualização da estratégia intitulada Estratégia Brasileira para a Transformação Digital (E-Digital) Ciclo 2022-2026 (BRASIL, 2022). A estratégia mantém o mesmo arranjo institucional e os mesmos eixos temáticos definidos pelo decreto 9.319/2018 que instituiu a estratégia E-digital em 2018.

Em termos do arranjo institucional, destaca-se a criação do Sistema Nacional para a Transformação Digital (SinDigital), composto pelo: (i) Comitê Interministerial para a Transformação Digital (CITDigital), com representantes de sete ministérios; (ii) Conselho Consultivo para a Transformação Digital, composto por especialistas e representantes da comunidade científica de notório saber, da sociedade civil e do setor produtivo, e (iii) demais órgãos, entidades e instâncias vinculados às políticas de transformação digital.

A Estratégia está dividida em dois eixos principais, subdivididos em subeixos:

(i) Eixos habilitadores: (i.1) Infraestrutura e acesso às tecnologias de informação e comunicação; (i.2) Pesquisa, desenvolvimento e inovação; (i.3) Confiança no ambiente digital; (i.4) Educação e capacitação profissional; (i.5) Dimensão Internacional;

(ii) Eixos de transformação digital: (ii.1) Transformação digital da economia, que inclui os temas (a) "Economia baseada em dados", (b) "Um Mundo de Dispositivos Conectados" e (c) "Novos Modelos de Negócio", e (ii.2) Cidadania e Transformação Digital do Governo.

[35] https://www.telesintese.com.br/com-nova-lei-da-preferencia-telebras-vai-entrar-no-mercado-de-data-center/

Em termos do subeixo de "infraestrutura e acesso às tecnologias de informação e comunicação", o diagnóstico atualizado reforça os mesmos aspectos destacados no documento de 2018: "segue sendo um elemento primordial para a transformação digital brasileira a ampliação da oferta do serviço de internet, somada à melhoria da qualidade e velocidade por todo o território. O Brasil possui diversos desafios para a extensão do acesso às redes de banda larga, sendo fundamental a ampliação da infraestrutura de redes de transporte de dados em fibra óptica para o escoamento de tráfego para os *backbones* nacionais.". O documento destaca o desafio diferenciado para a conexão de áreas do interior, áreas rurais e a população de menor nível de renda.

Com relação ao eixo "pesquisa, desenvolvimento e inovação", observa-se uma orientação estratégica parcialmente alinhada à diretriz de soberania digital discutida acima de 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços'. O eixo da estratégia destaca como objetivo geral "estimular o desenvolvimento de novas tecnologias, com a ampliação da produção científica e tecnológica, e buscar soluções para desafios nacionais". O documento faz referência aos instrumentos de fomento à inovação no país, com destaque para o desenvolvimento de startups e do empreendedorismo inovador. Também destaca a perspectiva de uso de encomendas tecnológicas e compras públicas para estimular o desenvolvimento de soluções adequadas aos desafios do país. Tal perspectiva é reforçada no subeixo "dimensão internacional", na medida em que a estratégia propõe objetivos específicos orientados ao fortalecimento das competências e empresas nacionais: "estimular a competitividade e a presença no exterior das empresas brasileiras com atuação nos segmentos digitais; promover a expansão de exportações por meio do comércio eletrônico e apoiar a inserção de pequenas e médias empresas brasileiras neste segmento".

Também no escopo do subeixo "confiança no ambiente digital" observa-se um alinhamento direto com diretrizes de promoção da soberania digital discutidos acima, destacadamente a 'segurança nacional e estado de direito' e 'autonomia dos usuários e autodeterminação individual'. O subeixo da estratégia destaca como objetivo geral "assegurar que o ambiente digital seja seguro, confiável e propício aos serviços e ao consumo, com respeito aos direitos dos cidadãos". Neste sentido, são de fundamental importância as diretrizes de "proteção de direitos no meio digital, inclusive nos aspectos relativos à privacidade e à proteção de dados pessoais" e de fortalecimento da "segurança cibernética" e "proteção da infraestrutura crítica", com papel destacado da Autoridade Nacional de Proteção de Dados (ANPD).

Tendo em vista o escopo da presente pesquisa, destaca-se a apresentação em documento oficial de política do Ministério de Ciência, Tecnologia e Inovação de uma conceituação para a Economia de Dados. O subeixo "Transformação digital da economia", destaca o tema "Economia baseada em dados". Uma perspectiva da conceituação, mesmo que não explícita, da economia de dados pode ser encontrada na seguinte passagem:

> "O reaproveitamento e a reutilização dos dados promovem o aumento recorrente de seu valor e faz com que se tornem um novo fator de produção, tal como bens materiais e capital humano. Ao mesmo tempo, os dados também impulsionam mudanças de sociabilidade, de modo que a sua mobilização se torna cada vez mais habitual e imprescindível.

> Desta forma, a produção de dados possui consequências diretas para a criação de novas oportunidades".

E também se apresenta uma identificação das tecnologias digitais que habilitam estes processos, ao se destacar o papel central dos dados enquanto insumos e produtos relacionados a tecnologias como "inteligência artificial, *machine learning*, realidade aumentada, *Big Data*, *cloud computing*, tecnologias biomédicas, entre outros campos relevantes para o desenvolvimento socioeconômico". O documento não apresenta nenhuma perspectiva de mensuração da economia de dados, apenas cita estimativas de volume global de tráfego na internet.

Portanto, de forma alinhada a diversas definições propostas pelo mundo, esta perspectiva destaca a: (a) geração de dados no âmbito de sociedade, estado e mercado, sua armazenagem e custódia; (b) a captura e processamento, análise de dados e produção de conhecimento. Por outro lado, não se observa no documento desta política um mapeamento das dimensões e mecanismos através dos quais podem ser dar o (c) consumo intermediário e (d) o consumo final de bens e serviços associados ao processamento dos dados e dos atores críticos nas diferentes etapas desta economia. Isto pode contribuir para um foco excessivamente centrado na adoção de tecnologias e na provisão de infraestrutura de base, sem ponderações sobre potenciais modelos de negócio e o papel de diferentes players na economia de dados.

Com efeito, uma perspectiva de soberania relacionada à 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços' é virtualmente ausente, na medida que as perspectivas de benefício para empresas e para a sociedade são vislumbradas maiormente pela adoção de tais tecnologias e não pelo desenvolvimento de competências tecnológicas e serviços no país. Isto fica evidente também nas discussão relacionadas aos subeixos "um mundo de dispositivos conectados" e "Plano Nacional de Internet das Coisas", ao se enfocarem apenas os potenciais benefícios decorrentes da adoção de tecnologias[36]. Também a menção ao imperativo de estabelecimento e ampliação de data centers e pontos de troca de tráfego no país faz alusão apenas genérica ao potencial de tais infraestruturas estimularem a atração e criação de empresas inovadoras. Por outro lado, a ausência de ponderações desta ordem na parte do documento que trata da economia de dados pode ser atenuada pelo fato de haverem, conforme indicado acima, menções nos subeixos "pesquisa, desenvolvimento e inovação" e "dimensão internacional" ao desenvolvimento de competências nacionais em tecnologias digitais.

O diagnóstico apresentado pelo documento contém uma orientação estratégica alinhada ao imperativo de soberania discutido acima de 'segurança nacional e defesa do estado de direito'. A perspectiva apresentada pelo documento do Ministério identifica os riscos inerentes aos processos de geração, tratamento e uso de dados e ressalta a importância de construção de estratégias ativas para seu adequado aproveitamento em prol do desenvolvimento: "volume crescente de dados não dá garantias de que seus efeitos serão benéficos. Esse crescimento exige

[36] Embora haja uma menção isolada ao reconhecimento de que "a disseminação de tais tecnologias é marcada por um padrão de desigualdade que tende a aumentar a distância entre países desenvolvidos, em desenvolvimento e pobres", esta perspectiva não se traduz em diretrizes de política.

um plano de ação que o qualifique, visando a circulação dos dados e sua recíproca fecundação em direção a serviços e produtos mais complexos, em um movimento consistente de desenvolvimento capaz de aumentar a renda brasileira nos prazos médio e longo". O documento preconiza a construção de "um sistema de dados nacionais integrados" que exige que seu "design considere os problemas de segurança, privacidade, integridade e eticidade que seu uso pode implicar". Ademais, o documento destaca ainda a importância de uma "governança de dados" e ressalta o importante papel a ser desempenhado pelo Comitê Central de Governança de Dados (CCGD)[37], contribuindo para reduzir "os riscos associados ao uso indevido de dados, a exemplo da vigilância política, de práticas monopolistas e anticompetitivas, espionagem e vazamento de dados pessoais ou sensíveis."

4.3.2 Programas de Política com Foco em Tecnologias Específicas

O Plano Nacional de Internet das Coisas foi instituído pelo Decreto nº 9.854, de 25 de junho de 2019, e tem como objetivo implementar e desenvolver a Internet das Coisas no País, com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais. Sua elaboração se deu a partir de uma parceria entre o MCTI e o BNDES.

A Estratégia Brasileira de Inteligência Artificial foi divulgada em julho de 2021, em alinhamento à Portaria MCTIC nº 1.122/2020, que definiu como prioridade a área de Inteligência Artificial, no que se refere a projetos de pesquisa, de desenvolvimento de tecnologias e inovações, para o período 2020 a 2023.

Ambas as estratégias fazem alusão à crescente importância dos dados enquanto matéria prima viabilizadora das respectivas tecnologias, mas não apresentam conceituação da economia de dados, tampouco uma visão minimamente estruturada dos vários processos e atores envolvidos. Os desdobramentos da importância dos dados para tais tecnologias se traduzem, sobretudo, em duas linhas de diretrizes. Em primeiro lugar, as orientações para a promoção de um ambiente de dados abertos se alinham sobretudo com as perspectivas de seu uso para alimentar sistema de Inteligência Artificial e os potenciais desdobramentos positivos de geração de valor por intermédio da aplicação de tais sistemas. Em segundo lugar, as diretrizes relacionadas à Infraestrutura de Conectividade e Interoperabilidade no Plano Nacional de Internet das Coisas buscam desenvolver os meios para a ampla circulação de dados. Ambas as estratégias não apresentam um reconhecimento do valor intrínseco aos dados e seu papel estratégico, limitando sua percepção de valor aos potenciais desdobramentos do emprego das respectivas tecnologias.

[37] O Comitê Central de Governança de Dados (CCGD) foi instituído pelo Decreto 10.046, de 9 de outubro de 2019, com competências para deliberar sobre as orientações e as diretrizes para a categorização de compartilhamento amplo, restrito e específico, referente à proteção de dados pessoais, bem como sobre as orientações e as diretrizes para a integração dos órgãos e das entidades com o Cadastro Base do Cidadão. Sua composição é dada por diversas secretarias e ministérios do executivo federal, do judiciários (CNJ), do legislativo (Senado e Câmara dos Deputados), além do Banco Central do Brasil, LAPIN - Laboratório de Políticas Públicas e Internet e GovDados - Governança de dados no setor público (https://www.gov.br/governodigital/pt-br/governanca-de-dados/comite-central-de-governanca-de-dados)

Outro aspecto comum às duas estratégias é a ausência de uma orientação de soberania digital e de dados relativa à "promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços". Eventualmente, por serem políticas gestadas dentro do MCTI, o foco no setor produtivo brasileiro fica restrito ao escopo de startups e do que tem sido chamado de "ecossistema de empreendedorismo", uma vez que o ministério possui incumbência de estímulo a estes empreendimentos. Assim, a estratégia em IA, por exemplo, dá os seguintes destaquem para a relação entre "Industrialização e IA: programas para incentivar a adoção de tecnologias em IA por parte do setor privado, com investimentos em setores estratégicos, financiamento para startups de IA, em pequenas e médias empresas, estratégias para criar clusters para IA".

Como fica evidente nesta citação, à parte estímulos a startups, não há nenhuma ponderação relativa a competências tecnológicas e inovativos no tecido produtivo mais amplo e as referências a estes se dão, essencialmente, pelo viés da adoção de tecnologias. A Estratégia Nacional em IA, em sua seção sobre aspectos internacionais, inicia chamando atenção para a corrida global pela liderança em IA, mas deixa evidente que não se vislumbra um papel para o sistema nacional de inovação nesta corrida, se limitando ao papel de adotante em setores de tradicionais vantagens competitivas estáticas: "Salienta-se que o Brasil vem priorizando os setores da economia em que já possui vantagem competitiva, a saber: agricultura, pecuária, mineração e indústria petroquímica".

Alinhado a esta visão bipartida – de um lado um rarefeito ecossistema de startups nestas tecnologias[38] e de outro um tecido produtivo com papel passivo de adotante – ambas as estratégias dão destaque para a importância de programas de cursos de formação e capacitação profissional e de graduação e pós-graduação alinhados a competências críticas nesta área e à formação de profissionais habilitados para viabilizar uma eficiente adoção e aplicação destas tecnologias no tecido produtivo.

Por fim, as estratégias apresentam um alinhamento relevante com uma orientação de soberania relacionada à "promoção de autonomia dos usuários e de autodeterminação individual". Especialmente a EBIA faz amplas ponderações e enumera diretrizes de ação relacionados ao "equilíbrio entre: (i) a proteção e a salvaguarda de direitos, inclusive aqueles associados à proteção de dados pessoais e à prevenção de discriminação e viés algorítmico", de forma que os sistemas desenvolvidos respeitem "os direitos humanos, os valores democráticos e a diversidade, impondo-se a inclusão de salvaguardas apropriadas que possibilitem a intervenção humana, sempre que necessária, para garantir uma sociedade justa" e evitem vieses algorítmicos.

Salienta-se, além do MCTI estar revisando a Estratégia de IA, que em março de 2024, em reunião do Conselho Nacional de Ciência e Tecnologia (CCT) sobre os avanços da IA no Brasil, o Presidente da República solicitou aos conselheiros que elaborem uma proposta de política de IA nacional, com o objetivo de tornar o país competitivo na área em nível mundial (Agência

[38] A EBIA afirma haverem apenas 26 startups no país com foco em Inteligência Artificial.

Gov, 2024). E declarou de modo contundente querer "uma IA genuinamente guarani" ou "yanomami" e instou pesquisadores a produzirem algo "nosso" (AMADEU, 2024).

No escopo das iniciativas específicas voltadas para alguns dos campos tecnológicos relacionados à economia de dados, cabe destacar o esforço de criação, em 2020, de uma rede de inovação envolvendo IA, Aprendizado de Máquinas, IoT, Big Data, Analytics, entre outras. A iniciativa capitaneada pelo MCTI e a Empresa Brasileira de Pesquisa e Inovação Industrial (Embrapii) articulou 17 instituições de pesquisa (unidades Embrapii) e destinou R$ 70 milhões para fomentar projetos de pesquisa e de formação de redes inovativas, incluindo startups. Outras iniciativas têm utilizado recursos do FNDCT para financiar projetos de pesquisa e inovação individuais, tais como o Programa IA² MCTI , a iniciativa de Centros de Pesquisa Aplicada (CPA) em IA , Finep IoT, encomendas tecnológicas como o programa Soluções de IA para o Poder Público, subvenção econômica no programa Finep Mais Inovação Brasil - Tecnologias Digitais , etc.

4.3.3 Estratégia Nacional de Governo Digital

O Decreto nº 10.332, de 28 de abril de 2020 (alterado pelos Decretos nº 10.996/ 2022 e nº 11.260/ 2022) institui a Estratégia de Governo Digital para o período de 2020 a 2023, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Os princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública estão definidos na Lei nº 14.129, de 29 de março de 2021 (Lei do Governo Digital).

A estratégia atualmente disponível, abrangendo o período de 2020 a 2023, engloba uma diversidade de frentes de atuação, sintetizados em seis eixos estratégicos associados a atributos do futuro governo digital: centrado no cidadão; integrado; inteligente; confiável; transparente e aberto; e eficiente.

Pode-se extrair uma perspectiva implícita de conceituação da economia de dados do documento da política, na medida em que indica que a "economia do presente é fortemente baseada no tratamento e uso de dados e o Estado detém e armazena uma parte relevante desses dados". O potencial valor para o governo e o para a sociedade fica evidente ao se indicar que "uma plataforma tecnológica para análise, curadoria, descoberta, mineração e integração de informações governamentais possibilita o cruzamento de dados e uma análise estratégica para a tomada de decisão e assertividade na destinação dos recursos públicos dos programas sociais." [39]

Com relação à mensuração da economia de dados, só se verifica uma perspectiva indireta relacionada à medição da economia de recursos proporcionada pela transformação digital do governo. No site da estratégia[40], constam como concluídas a "iniciativa 17.1: Aprimorar metodologia de medição da economia de recursos com a transformação digital até 2020" e a "iniciativa 17.2: Disponibilizar painel com o total de economia de recursos aferida com a transformação digital até 2020". Contudo, não foi possível identificar no site do governo e,

[39] https://www.gov.br/governodigital/pt-br/EGD2020/inteligente
[40] https://www.gov.br/governodigital/pt-br/EGD2020/eficiente

especificamente, no site do Ministério da Gestão e da Inovação em Serviços Públicos o detalhamento de tal metodologia, tampouco o painel com a economia de recursos.

Considerando os principais meios para tornar realidade este potencial de geração de valor, o documento destaca inúmeras iniciativas relacionadas a dados em poder do poder público, tais como "catalogar, no mínimo, as 300 principais bases de dados do Governo federal até 2022" e promover "um barramento de interoperabilidade de dados que facilite a integração e o reuso dessas informações para a prestação de serviços aos cidadãos".[41] Neste segundo objetivo, destaca-se a articulação do Cadastro Base do Cidadão[42], instituído pelo Decreto nº 10.046 de 9 de Outubro de 2019, com o Cadastro Nacional de Pessoa Jurídica e cm o Cadastro de Endereçamento Postal até 2022. Se insere neste escopo também o acesso digital único aos servidores públicos federais, a consolidação de 622 domínios do Poder Executivo federal no portal único gov.br, até 2022 e o uso, por todos os cidadãos, de um login único de acesso gov.br para 1.000 serviços públicos digitais, até 2022 e estabelecer 15 cadastros base de referência para interoperabilidade do Governo federal até 2023.

A estratégia não apresenta nenhuma perspectiva dos elos críticos da cadeia de valor da economia de dados ou do conjunto de atores do sistema produtivo e inovativo da economia de dados, o que sugere uma orientação circunscrita ao uso de dados dos indivíduos e empresas por parte de órgãos do próprio governo, sem que estes impulsionem atividades econômicas com fins de lucro. Contudo, tal perspectiva não se sustenta ao se analisar as diversas iniciativas relacionadas ao macro-objetivo "inteligente" e "eficiente". As iniciativas "8.2: Implementar recursos de inteligência artificial em, no mínimo, 12 serviços públicos federais até 2022"[43] e "8.3: Disponibilizar, pelo menos, 9 conjuntos de dados por meio de soluções de blockchain na administração pública federal até 2022" não fazem nenhuma referência à mobilização de competências dentro do próprio governo ou órgãos vinculados, deixando em aberto a perspectiva de contratação destes serviços junto a fornecedores privados de serviços.

Por outro lado, as iniciativas "8.4: implementar recursos para criação de uma rede blockchain do Governo federal interoperável, com uso de identificação confiável e de algoritmos seguros"[44] e "8.5: Implantar um laboratório de experimentação de dados com tecnologias emergentes até 2023" sugerem a mobilização de competências existentes no país.

---

[41] https://www.gov.br/governodigital/pt-br/EGD2020/integrado

[42] A estratégia prevê também a ampliação para 20 do número de atributos no cadastro base do cidadão até 2023, tornando a base mais rica e, ao mesmo tempo, mais crítica e estratégica, tendo em vista o grande número de parâmetros organizados em base estruturada sobre os cidadãos brasileiros.

[43] Como desdobramento do uso de tal tecnologia, a estratégia indica as iniciativas "9.1: Implantar mecanismo de personalização da oferta de serviços públicos digitais, baseados no perfil do usuário, até 2022" e "9.2: Ampliar a notificação ao cidadão em, no mínimo, 25% dos serviços digitais".

[44] Além de iniciativas individuais de diversos órgãos vinculados ao governo, destaca-se o acordo de cooperação técnica assinado pelo Tribunal de Contas da União (TCU) e o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em maio de 2022, para a criação da Rede Blockchain Brasil (RBB). Objetiva-se a criação de uma rede pública e sem fins lucrativos, de abrangência nacional, conectando instituições participantes em uma estrutura de governança e infraestrutura tecnológica voltadas para soluções de interesse público (https://portal.tcu.gov.br/imprensa/noticias/tcu-e-bndes-lancam-rede-blockchain-brasil-nesta-segunda-feira.htm).

Tomando as quatro grandes linhas de objetivos relacionados à soberania digital e de dados, discutidos acima, a análise do documento sugere que não são levados adequadamente em consideração a 'segurança nacional e defesa do estado de direito e a 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços'. Se por um lado há a indicação de projetos para o desenvolvimento de infraestruturas e soluções tecnológicas próprias, a maioria das iniciativas primam pela lógica da adoção das tecnologias em questão, na medida em que apresentam metas ambiciosas de ampliação de seu uso no curto prazo.

Os riscos potencias a uma perspectiva sólida de segurança nacional e a limitada preocupação com o desenvolvimento de competências nacionais ficam ainda mais evidentes ao se considerar as iniciativas sob a macro-meta da estratégia denominada "eficiente". O diagnóstico reconhece que a "órgãos da Administração Pública Federal possuem mais de 130 datacenters, com inúmeras oportunidades de otimização, além de fragilidades associadas à disponibilidade e segurança". A partir deste diagnóstico se desdobram duas iniciativas na estratégia. Em primeiro lugar, "16.4: Otimizar a infraestrutura de, pelo menos, 30 datacenters do governo até 2022". E, em segundo lugar, "16.5: Migração de serviços de, pelo menos, 30 órgãos para a nuvem até 2022". É notório que a inciativa de otimização de datacenters do governo foi revogada, ao passo que a de migração de serviços para serviços de computação em nuvem consta como concluída no site da estratégia[45]. Evidencia-se uma opção explícita de utilização de pacotes de serviços fornecidos por grandes corporações internacionais de tecnologia, colocando um risco um volume significativo de dados sensíveis dos cidadãos e do próprio governo.

Os Box 2 e 3 ilustram bem este panorama nos casos do judiciário federal, do Ministério da Educação e da Plataforma Sougov.

Box 2 – Serviços Tecnológicos no Judiciário Brasileiro

Em fevereiro de 2019, um anúncio do Poder Judiciário do estado de São Paulo indicava o plano de armazenamento e processamento dos processos judiciais no serviço de computação em nuvem da Microsoft. De forma associada, a intenção era de agregação de serviços de inteligência artificial para facilitar o registro, o arquivamento e a tramitação de todos os processos[46]. De acordo com o tribunal: "ao final de cinco anos, o custo fixo anual do TJ com o sistema judicial teria redução de 40%, além de eliminar a necessidade de alto investimento na renovação de Data Center"[47]. Conforme explicita Silveira (2021), virtualmente nenhum veículo, colunista ou parlamentar problematizou a "entrega" dos dados dos processos civis, criminais, empresariais, de crianças e adolescentes, para uma Big tech com claros interesses econômicos e políticos no país. Contudo, afortunadamente, o Conselho Nacional de Justiça (CNJ) proibiu a execução do contrato[48].

[45] https://www.gov.br/governodigital/pt-br/EGD2020/eficiente

[46] https://www.valor.com.br/legislacao/6128767/processos-do-tj-sp-serao-armazenados-na--nuvem; https://computerworld.com.br/negocios/tjsp-fecha-contrato-de-r-13-bi-com-microsoft-para-plataforma-digital/"

[47] https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=55845

[48] https://www.cnj.jus.br/plenario-ajusta-liminar-que-regula-contrato-do-tjsp-com-microsoft/

Porém, em oposição a preocupações que poderiam fundamentar a decisão, relacionados à soberania de dados (em termos da proteção de dados sensíveis da população e/ou em termos da promoção de competências nacionais em IA), o motivo destacado foi a intenção do CNJ de promover o desenvolvimento integrado de soluções para a digitalização e tramitação de processos no país como um todo.

A ausência de uma reflexão mínima acerca dos desafios da colonização de dados fica evidente em anúncio recente que dá corpo às intenções de desenvolvimento integrado pelo CNJ. Em 17 de Outubro de 2023, o ministro Luís Roberto Barroso, em sua primeira sessão como presidente do Conselho, relatou que encomendou às *Big Techs* (Amazon, Microsoft e Google) o desenvolvimento de soluções para agilizar e integrar digitalmente as atividades do judiciário do pais: (i) um programa capaz de resumir os principais elementos dos processos; (ii) uma ferramenta de inteligência artificial generativa para uso estritamente jurídico, alimentada com jurisprudência dos tribunais brasileiros e capaz de indicar/sugerir decisões, supervisionadas pelo juiz do caso; (iii) uma interface única que permita a interoperabilidade dos sistemas judiciais eletrônicos de todos os tribunais. A segunda das soluções supostamente poderia ser disponibilizada em 8 semanas, teriam afirmado os dirigentes das empresas consultadas. Na mesma fala, o ministro também anunciou a disponibilidade de R$ 28 milhões para fomentar o aperfeiçoamento da tecnologia da informação que serve ao judiciário brasileiro. Tendo em vista a indicação do juiz, tais recursos estão mais pertos de tais Big Techs, na medida em que atendam às encomendas feitas, do que de eventuais desenvolvedores, empresas ou instituições de pesquisa nacionais[49].

Box 3 – Serviços Tecnológicos na Educação

Em 2020, o Ministério da Educação contratou os serviços de computação em nuvem da Microsoft, chamada Azure, para receber e processar os dados do Sistema de Seleção Unificada (SiSU).

Desta forma, uma ampla gama de dados pessoais - renda familiar bruta mensal de cada um, os valores recebidos em diversos programas sociais, a nota no Enem, as médias populacionais relacionadas à cor declarada e a deficiências, entre outras informações sensíveis - de milhões de brasileiros passaram a ser processados em servidores de uma empresa estrangeira de um país que não possui legislação alinhada à LGPD.

Conforme relata Silveira (2021), o argumento principal apresentado pelo MEC foi o alto custo para processar estes dados em um data center de órgão vinculado ao governo. Os gestores apontam a expectativa de que a opção feita gere uma economia de aproximadamente 22 milhões de reais em cinco anos de projeto. Outro argumento seria de que a opção pelo prestador de serviço estadunidense contribuiria para aumentar a ‘segurança’ do processo, contudo sem uma definição de o que se entende por segurança neste contexto.

[49] https://www.migalhas.com.br/quentes/395504/barroso-pede-a-big-techs-criacao-de-chatgpt-para-uso-juridico

Conforme conclui Silveira (2021)[50]:

> No contexto da governamentalidade neoliberal, a construção de uma solução infraestrutural para a hospedagem de dados e a implementação de frameworks de inteligência artificial do próprio MEC e das universidades brasileiras não é considerada razoável. A economia imediata, a entrega de atividades antes executadas pelo Estado a empresas privadas, a crença em contratos e em um padrão moral isento de interesses geoestratégicos e negociais conformam um regime de verdade da gestão pública neoliberal.

A estratégia traz como um dos seus eixos centrais a promoção de "um governo transparente a aberto", em alinhamento com o decreto nº 8.777/2016, que institui a Política de Dados Abertos do Poder Executivo Federal. Desta forma, destaca as plataformas transparencia.gov.br e dados.gov.br que viabilizam o acesso a mais de 7 mil conjuntos de dados. A estratégia explicita como dados abertos podem servir para a alimentação de sistemas de Inteligência Artificial e o desenvolvimento de outras tecnologias e soluções potencialmente úteis para o governo. Nesta linha, figuram as iniciativas, assinaladas como concluídas, de "Ampliar a quantidade de bases de dados abertos"; "Melhorar a qualidade das bases de dados abertos".

Retomando as grandes linhas de objetivos relacionados à soberania digital e de dados, discutidos acima, a análise do documento contempla, em grande medida, aspectos relacionados a 'promoção de autonomia dos usuários e de autodeterminação individual', na medida em que ressalta a importância da privacidade do cidadão, o imperativo de adequação de plataformas à LGPD e de implementação de controles de segurança cibernética[51].

Destacam-se as seguintes iniciativas da estratégia, que constam no site da estratégia como concluídas em outubro de 2023: "11.2: implementar controles de segurança da informação e privacidade em 30 sistemas críticos do Governo federal, até 2022"; 11.3: definir padrão mínimo de segurança cibernética a ser aplicado nos canais e nos serviços digitais, até 2022"; "12.1: prover 2 milhões de validações biométricas mensais para serviços públicos federais, até o final de 2020."; "12.2: disponibilizar identidade digital ao cidadão, com expectativa de emissão de 40 milhões, até 2022" e "12.4: Disponibilizar novos mecanismos de assinatura digital ao cidadão, até 2022" .

A estratégia de Governo Digital está sendo atualizada através de uma sistemática ampla de consultas públicas, conduzida pelo Ministério da Gestão e Inovação em Serviços Públicos (MGI), com o apoio de diversos parceiros, dentre os quais o Conselho Nacional de Secretários de Estado de Administração (Consad) e a Frente Nacional de Prefeitos (FNP). O cronograma da estratégia previa o lançamento do documento atualizado para o mês de novembro de 2023, mas tal evento não ocorreu até a data de conclusão da redação deste relatório.

No escopo da estratégia de governo digital, cabe também destacar a iniciativa da Rede Nacional de Governo Digital (Rede GOV.BR), através da qual o governo federal busca apoiar estados e

[50] https://www.sul-sur.com/2023/09/soberania-digital.html
[51] https://www.gov.br/governodigital/pt-br/EGD2020/confiavel

municípios a avançarem na digitalização. Em novembro de 2023 a rede abarcava os 26 estados e o Distrito Federal e 512 municípios. A iniciativa oferece mecanismos de autodiagnóstico do grau de avanço da digitalização, orientação e guias para a construção de uma agenda, além de possibilitar que estados e municípios usem soluções tais como o login único, a assinatura eletrônica e a prova de vida digital, através da plataforma gov.br.[52]

Uma iniciativa para a conscientização da importância dos dados para a gestão pública se deu com o 4º Fórum de Governança de Dados em novembro de 2023. O evento teve como foco ampliar a percepção da importância da estruturação de catálogos de dados, para que os dados produzidos pelos diversos órgãos públicos possam ser encontrados e utilizados à serviço da entrega de serviços mais eficientes para a população.

4.3.4 Política Nacional de Segurança da Informação

A Política Nacional de Segurança da Informação foi instituída pelo Decreto nº. 9.637 de 26 de dezembro de 2018, alterado pelo Decreto nº 10.641 de 2 de março de 2021, prevendo a criação de uma Estratégia Nacional de Segurança da Informação. O Decreto explicita, dentre os princípios orientadores, diversos que apresentam um alinhamento direto com uma perspectiva de soberania digital e de dados centrada na "segurança nacional e na defesa do Estado de Direito":

> "Art. 3º São princípios da PNSI: I - soberania nacional; [...] VIII - orientação à gestão de riscos e à gestão da segurança da informação; IX - prevenção e tratamento de incidentes de segurança da informação; X - articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação; XI - dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas".

Para gerir a política, o decreto institui o Comitê Gestor da Segurança da Informação, com atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República nas atividades relacionadas à segurança da informação. Para definir estratégias operacionais, o decreto determina a elaboração de estratégias específicas relacionadas aos seguintes módulos: I - segurança cibernética; II - defesa cibernética; III - segurança das infraestruturas críticas; IV - segurança da informação sigilosa; e V - proteção contra vazamento de dados. Contudo, até o momento, apenas foram definidos a Estratégia Nacional de Segurança Cibernética (E-Ciber) e o Plano Nacional de Segurança de Infraestruturas Críticas.

A Estratégia Nacional de Segurança Cibernética - E-Ciber foi instituída pelo Decreto nº 10.222, de 5 de fevereiro de 2020. Dado seu escopo, é inerente o alinhamento com uma orientação de

[52] https://plataforma.rede.gov.br/

soberania digital e de dados orientada para a "segurança nacional e defesa do estado de direito". Em seu diagnóstico, o documento destaca a

> "importância de instrumentos normativos adequados à realidade brasileira que, de fato, contribuam para a proteção dos sistemas e de redes governamentais, uma vez que os serviços apoiados nesses recursos não podem sofrer interrupções, vazamento de dados ou serem alvos de outras ações danosas".

A potencial vulnerabilidade de infraestruturas e serviços críticos é reconhecida:

> "outro ponto crítico refere-se à proteção cibernética das empresas representantes das infraestruturas críticas. A título de compreensão, podemos conceituá-las como as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional".

Nesta linha, são exploradas as diversas frentes de ação que devem contribuir para a segurança cibernética. No que se refere à dimensão normativa, a estratégia destaca a necessidade de complementação do quadro legal, constituindo uma lei específica sobre segurança cibernética. No que se refere à Pesquisa, Desenvolvimento e Inovação, o documento da estratégia apresenta uma perspectiva abrangente da indústria nacional ao indicar que "é preciso que o país disponha de uma indústria de segurança cibernética inovadora, apoiada por pesquisas e por produções científicas de alto nível, capaz de reter talentos que possam contribuir com a indústria nacional e realimentar o ciclo de produção do conhecimento". Contudo, posteriormente circunscreve, a exemplo de outras estratégias analisadas, o escopo do potencial inovativo às startups: "startups desempenham papel de relevância como principais fontes de inovação. A percepção de seu potencial inovador incentivou diversos países a estabelecerem ampla gama de programas de apoio a startups e a pequenas e médias empresas, solução que o Brasil deve seguir e incentivar".

A concepção do grosso do tecido produtivo como espaço de aplicação de tecnologias críticas, e não como locus de mobilização de competências para seu desenvolvimento, fica evidente também na seção que trata sobre Dimensão Internacional e Parcerias Estratégicas, ao listar as tecnologias e seus potenciais impactos positivos, mas sem conceber o potencial de empresas situadas no país se constituírem como *players* no desenvolvimento de soluções baseadas nestas tecnologias.

No que concerne o eixo educação, além do esperado foco na formação técnica e superior relacionada à segurança cibernética, destaca-se a proposição de um conjunto de iniciativas alinhadas a uma perspectiva de soberania centrada na "promoção de autonomia dos usuários e de autodeterminação individual":

> "Nesse contexto, destaca-se a importância da alfabetização digital, ou *digital literacy*, [...], significa "possuir as habilidades necessárias para viver, aprender e trabalhar em uma sociedade em que a comunicação e o acesso à informação ocorrem cada vez mais por meio de tecnologias digitais, como plataformas da Internet, mídias sociais e dispositivos móveis".

Por fim, cabe destacar que a segurança cibernética é abordada na estratégia exclusivamente pelo prisma da prevenção, proteção e reação a atos mal-intencionados e/ou ilegais (os ilícitos cibernéticos). Não se discute a segurança de dados sob o prisma das escolhas de localização para o armazenamento de dados críticos ou de que prestadores de serviços são mobilizados para processar estes dados para a provisão de serviços (e em que medida os respectivos países possuem legislação de proteção de dados alinhada à LGPD). É esvaziada, desta forma, qualquer preocupação de ordem estratégica e geopolítica, como o risco de compartilhamento e venda de dados críticos de cidadãos brasileiros e seu uso para treinar algoritmos de IA ou a espionagem e manipulação política, etc. Assim, A estratégia concebe os atores e prestadores de serviços formais em todo o globo como igualmente bem intencionados e alinhados aos parâmetros legais e regulatórios implementados no Brasil, a despeito dos inúmeros casos recentes de uso indevido de dados por agências de inteligências e grandes corporações estrangeiras.

O decreto nº 11.856, de 26 de dezembro de 2023 formaliza a Política Nacional de Cibersegurança – PNCiber. Considerando as diretrizes orientadoras, o decreto apresenta um importante avanço com relação à E-ciber, ao destacar como principal diretriz não somente a "soberania nacional", mas também a "priorização dos interesses nacionais". Esta perspectiva de "interesses nacionais" pode ser interpretada sob o prisma da promoção de uma soberania nacional em termos da 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços'. Reforça tal perspectiva o fato de ser citado como primeiro objetivo da política "promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética".

Considerando a orientação de soberania relacionada à 'segurança nacional e defesa do estado de direito', o documento também apresenta algum avanço importante. Além de considerar o "combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço", o documento também explicita como quinto objetivo "estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos". Embora não seja explicitado no documento, tal colocação abre espaço para que se questione em que medida a natureza dos atores envolvidos, os parâmetros e a localização dos serviços de armazenagem e processamento em nuvem, etc. podem ser considerados como potenciais elementos de vulnerabilidade. De toda forma, tal objetivo abre escopo para a consideração mais ampla e estratégica do ciberespaço e dos potenciais riscos para a soberania nacional.

O documento avança para além dos objetivos discutidos, mas elenca a E-ciber como elemento constituinte da política nacional de cibersegurança. Mas a E-ciber também se limita a diretrizes de ação pouco operacionais. Por outro lado, o decreto institui o Comitê Nacional de Cibersegurança – CNCiber, com representantes dos mais diversos ministérios e outros atores, reconhecendo o caráter transversal da matéria e estabelecendo o fórum ideal para que sejam mobilizados ações e instrumentos concretos para que sejam atingidos os objetivos apontados.

4.3.5 Plano Nova Indústria Brasil

Em janeiro de 2024, foi lançado pelo Ministério do Desenvolvimento, Indústria e Comércio o documento do plano de ação da estratégia Nova Indústria Brasil, referência para a política industrial e de inovação do país para o período 2024-2026. É inquietante que o documento não reconheça explicitamente a Economia de Dados como um espaço de geração de valor substancial, com crescente relevância futura. Por outro lado, há importantes referências e proposição de ações concretas com relação à transformação digital e a tecnologias que possuem interface com a Economia de Dados.

A primeira importante referência está na missão relacionada ao Complexo Econômico Industrial da Saúde e ao SUS, onde se explicita o objetivo específico de "desenvolver tecnologias da informação e da comunicação, com domínio nacional de dados[...]". A segunda referência se dá na missão relacionada a infraestrutura, saneamento, moradia e mobilidade. Associado ao objetivo específico de "ampliar infraestruturas digitais locais com foco em conectividade de alta velocidade e resiliente", identifica-se a iniciativa de apoio à ciber-infraestrutura nacional, por intermédio da Estratégia Nacional de Datacenters e serviços de computação em nuvem, a qual se propõe a incentivar a implantação e expansão em território nacional de Datacenters seguros e sustentáveis, o fomento de serviços de computação em nuvem com conhecimento e tecnologias desenvolvidas no país.

Por fim, identifica-se um conjunto de referências relacionadas à missão de transformação digital da indústria. Três dos objetivos específicos se alinham diretamente com uma diretriz de promoção da soberania associada à 'autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços', ao objetivarem desenvolver empresas nacionais competitivas em tecnologias digitais disruptivas e emergentes e o aumento da participação de empresas nacionais no segmento de plataformas digitais. Enquanto este último item figura apenas como intenção abstrata, o primeiro encontra repercussão na indicação de instrumentos concretos, com destaque para a indicação de "tecnologias digitais disruptivas" (e.g. IA Generativa, tecnologias quânticas, segurança cibernética, blockchain) como prioridade para a destinação de recursos não reembolsáveis de promoção da inovação (previsão de R$ 260 milhões). Ademais, identificam-se ações pontuais, como o programa Startup GOV.BR, com destinação de R$ 36 milhões para a contratação de nove projetos em "tecnologias disruptivas".

Observa-se, ainda, uma perspectiva alinhada à soberania nacional pelo prisma da segurança nacional no projeto de estabelecimento da Rede Privativa de Comunicação da Administração Pública Federal até 2026, constituindo infraestrutura segura para atender atividades de missão crítica, como segurança pública, defesa, serviços de emergência, resposta a desastres e outras atribuições críticas do Estado.

Considerações Finais

O estudo buscou traçar um panorama das conceituações e perspectivas de mensuração da economia de dados o Brasil, considerando diferentes organizações e o marco legal relevante. Em vez de uma análise puramente técnica e factual, o estudo buscou orientar a análise por um

referencial conceitual e analítico. Tal estratégia se fundamenta no seguinte fato: conceitos não são neutros. Eles são politicamente, socialmente e culturalmente condicionados e carregam consigo implicações em termos dos marcos legal e institucional erigidos em torno de si e em termos das políticas públicas explícitas e implícitas.

Neste sentido, é fundamental considerar que um conceito de 'economia de dados' útil e adequado a uma diretriz de desenvolvimento do Brasil precisa levar em consideração preceitos amplos de soberania, os condicionantes específicos a um país em desenvolvimento e uma perspectiva sistêmica, conforme cunhada por autores e instituições do sul global.

De forma geral, a análise revelou um estágio ainda inicial do reconhecimento da importância da economia de dados para a economia e a sociedade brasileira, com um marco legal em contínua construção e a ausência de iniciativas estruturadas de mensuração desta economia.

No que diz respeito ao IBGE, órgão coordenador do sistema nacional de estatísticas, ficou evidente que o órgão ainda não adota uma conceituação de Economia de Dados e que ainda não foram mobilizados esforços para a sua mensuração direta. Apenas esforços de conceituação e mensuração do escopo mais amplo e difuso da economia digital têm sido mobilizados. De forma complementar, as pesquisas realizadas pelo CETIC.br contemplam as dimensões de adoção de tecnologias digitais em diferentes setores e esferas da sociedade.

Portanto, tanto o IBGE quanto o CETIC.br não apresentam uma conceituação explícita de 'economia de Dados', se alinhado a uma perspectiva ampla de Economia Digital e digitalização da economia. Contudo, sob o ponto de vista da cadeia de valor da economia de dados propriamente dita, os estudos não enfocam e não detalham atores e atividades relacionadas ao ciclo de valor.

Perspectivas atuais do IBGE apontam para um reconhecimento maior da relevância da economia de dados, ao mobilizar esforços para a constituição de um *data lake*, a partir das diversas bases de dados de diferentes órgãos públicos e o desenvolvimento de ferramentas de inteligência artificial, de forma a viabilizar o uso estratégico destes dados na pesquisa, elaboração, implementação e avaliação de políticas públicas.

No que se refere ao marco legal, a pesquisa destacou a robustez e abrangência dos preceitos fundamentais presentes na Constituição Federal, a qual contempla, de forma articulada, todas as quatro dimensões da soberania nacional orientadoras deste estudo. Uma perspectiva ampla de soberania nacional se articula com sua manifestação na esfera econômica e o papel do mercado interno e do desenvolvimento científico e tecnológico. Os dispositivos relacionados aos direitos fundamentais subordinam a ordem política e econômica à garantia de autodeterminação individual e à proteção da identidade e diversidade sociocultural do país. E os imperativos da ordem econômica e de atuação do Estado estão subordinados ao objetivo fundamental do desenvolvimento do país.

No que se refere às leis relacionadas à economia de dados, destacou-se o Marco Civil da Internet, a LGPD e projetos de lei. No que se refere à conceituação da economia de dados, a LGPD apresenta uma perspectiva ampla do Sistema Produtivo e Inovativo na Economia de Dados, contemplando a diversidade de atores relevantes, sistematizando os principais papeis

que podem ser exercidos por diversos atores, tais como provedores de serviços online e plataformas digitais no tratamento de dados pessoais.

As duas leis preconizam claramente uma orientação para a uma perspectiva de soberania relacionada a 'autonomia dos usuários e de autodeterminação individual', ao buscar estabelecer e defender direitos fundamentais dos indivíduos no meio cibernético e também ao vislumbrar o importante papel de iniciativas de educação e capacitação para dotarem os indivíduos de ferramentas para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania.

No que concerne a diretriz de soberania relacionada à 'segurança nacional e defesa do estado de direito', a LGPD determina, por exemplo, o tratamento direto por órgão vinculado ao Estado e em território nacional de dados críticos à segurança nacional. Na mesma linha, destaca-se a limitação imposta pela lei para a transferência internacional de dados pessoais e seu processamento no exterior. Em tese, a lei proíbe tal transferência e processamento em países que não possuam um marco legal alinhado à LGPD, excluindo por exemplo os EUA. Mas, por outro lado, a lei apresenta um afrouxamento excessivo, na medida em que exige apenas que preceitos alinhados à lei constem em contratos particulares de prestação de serviços, mesmo sem que exista capacidade de *enforcement* internacional para o cumprimento de tais cláusulas.

As demais dimensões de objetivos relativos à soberania digital e de dados não encontram repercussão relevante no Marco Civil da Internet e são parcialmente contempladas na LGPD. Destacadamente, uma orientação para a 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços' se mostrou virtualmente inexistente nestas leis.

O projeto de lei complementar que busca instituir a Lei Geral de Empoderamento de Dados, se propõe a fechar muitas destas lacunas. O projeto propõe uma conceituação mais elaborada do SPID no que denomina de Ecossistema Brasileiro de Monetização de Dados. Contudo, embora o projeto constitua importante avanço sob o ponto de vista da promoção de 'autonomia dos usuários e de autodeterminação individual', o mesmo não contempla as demais dimensões de soberania consideradas relevantes. Não há considerações sobre aspectos de 'segurança nacional' e a natureza especialmente crítica de dados relacionados a diversos sistemas e infraestruturas vitais para a sociedade. Embora proponha um conjunto de dispositivos para regulamentar e regular o mercado de dados no país, não se observa nenhuma orientação relacionada à natureza e origem dos atores e tecnologias empregadas, negligenciando uma perspectiva de soberania relacionada à 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços'. Tampouco são contemplados aspectos relacionados à 'proteção da identidade e diversidade sociocultural, promovendo a proteção do patrimônio cultural, a diversidade linguística'.

A discussão acerca das orientações presentes no quadro jurídico e normativo sobre a possibilidade de órgãos públicos contratarem serviços de computação em nuvem do exterior se mostrou dúbia ou inconclusa. Tal prática não é vedada nas leis relevantes, mas os dispositivos infralegais sugerem que devam ser priorizados os provedores nacionais e públicos destes serviços. A questão resulta dependente de uma apreciação sujeita a subjetividades sobre a

capacidade efetiva de organizações públicas, como Serpro e DataPrev, etc., atenderem as demandas colocadas pelos diversos órgãos.

Também foram considerados os principais documentos de políticas públicas em áreas que possuem interface com a economia de dados.

A Estratégia Brasileira para Transformação Digital (E-digital) traz importante reconhecimento da importância estratégica dos dados e de seu processamento e o reconhecimento de que um volume crescente de dados não garante, por si, efeitos benéficos par aa socioeconomia do país. O documento da estratégia apresenta uma conceituação implícita de economia de dados, ao destacar a forma como o reaproveitamento e a reutilização dos dados promovem o aumento recorrente de seu valor, ao reconhecer as mudanças nos padrões de sociabilidade e novas oportunidades abertas por esta economia. Contudo, o foco é restrito aos processos de geração, armazenagem e custódia, processamento, análise de dados e produção de conhecimento, não explorando as formas de consumo intermediário e consumo final de bens e serviços associados ao processamento dos dados e dos atores críticos nas diferentes etapas desta economia. Isto pode contribuir para um foco excessivamente centrado na adoção de tecnologias e na provisão de infraestrutura de base, sem ponderações sobre potenciais modelos de negócio e o papel de diferentes players na economia de dados.

Sob o ponto de vista de seu foco e suas implicações para a soberania, a E-digital se apresenta relativamente vaga e omissa. À exemplo das leis analisadas, o principal foco reside em uma perspectiva de soberania relacionada à 'autonomia dos usuários e autodeterminação individual', objetivando constituir um ambiente digital seguro, confiável e propício aos serviços e ao consumo, com respeito aos direitos dos cidadãos. No que se refere à diretriz de soberania relacionada à 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços', a estratégia se limita a uma perspectiva de estímulo ao desenvolvimento de novas tecnologias, com a ampliação da produção científica e tecnológica, enfatizando o papel de startups.

Outras políticas com foco em tecnologias específicas, tais como o Plano Nacional de Internet das Coisas e a Estratégia Brasileira de Inteligência Artificial não apresentam uma conceituação explícita ou implícita de economia de dados, tampouco uma visão minimamente estruturada dos vários processos e atores envolvidos. Também estas políticas trazem uma ênfase excessiva na adoção de tecnologias em detrimento de uma orientação para o desenvolvimento de competências nacionais no desenvolvimento destas tecnologias. Eventualmente, por serem políticas gestadas dentro do MCTI, o foco no setor produtivo brasileiro fica restrito ao escopo de startups e do que tem sido chamado de "ecossistema de empreendedorismo". Não há nenhuma ponderação relativa a competências tecnológicas e inovativos no tecido produtivo mais amplo e as referências a estes se dão, essencialmente, pelo viés da adoção de tecnologias.

Esta perspectiva bipartida presente na E-digital e nas demais políticas – de um lado, um rarefeito ecossistema de startups nestas tecnologias e, de outro, um tecido produtivo com papel passivo de adotante – poderia ser amenizada pela presença de uma estratégia robusta de política industrial e de inovação. Contudo, um ano após o início da atual gestão do governo federal, tal política ainda segue em fase de elaboração, tornando o prazo para sua futura implementação sensivelmente exíguo.

Situação idêntica se aplica à estratégia nacional de governo digital, que também ainda não foi divulgada, de forma que o documento teoricamente vigente é a estratégia publicada em 2020 abrangendo o período de 2020 a 2023. O documento da estratégia apresenta um reconhecimento de que a economia do presente é fortemente baseada no tratamento e uso de dados e o Estado detém e armazena uma parte relevante desses dados. O potencial valor para o governo e o para a sociedade é associado à potencial análise estratégica para a tomada de decisão em matéria de políticas públicas. Contudo a estratégia também não traz um reconhecimento dos elos críticos do ciclo de valor da economia de dados ou do conjunto de atores do sistema produtivo e inovativo da economia de dados, o que sugere uma orientação circunscrita ao uso de dados dos indivíduos e empresas por parte de órgãos do próprio governo, sem que estes impulsionem atividades econômicas. A referência a iniciativas em matéria de inteligência artificial e *blockchain* aplicados à gestão pública, não consideram adequadamente a mobilização de competências dentro do próprio governo ou órgãos vinculados, deixando em aberto a perspectiva de contratação destes serviços junto a fornecedores privados de serviços, eventualmente estrangeiros. Casos como o do CNJ e do SiSU no MEC evidenciam esta orientação. Por outro lado, observam-se também importantes iniciativas em curso a partir de parcerias entre ICTs brasileiras e órgãos públicos para o desenvolvimento e emprego de soluções baseados nestas tecnologias.

Por fim, o estudo contemplou também a estratégia e a política de segurança da informação. Destaca-se um alinhamento com uma perspectiva de soberania centrada na 'segurança nacional e na defesa do Estado de Direito', centrados no imperativo de proteção dos sistemas e de redes governamentais. Uma orientação mais estratégica fica evidente ao se buscar prevenir, evitar e mitigar vulnerabilidades, o que pode trazer implicações relativas ao uso de serviços baseados em empresas e infraestruturas no exterior, sobretudo em países com legislação não alinhada à LGPD.

A estratégia sublinha uma orientação para os "interesses nacionais", que se associam com a 'promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços'. Tal diretriz fica evidente na medida em que a estratégia propõe o desenvolvimento de uma indústria nacional de segurança cibernética inovadora, apoiada por pesquisas e por produções científicas de alto nível, contribuindo com a indústria nacional e realimentando o ciclo de produção do conhecimento no país.

Conclui-se que o país ainda não possui uma conceituação consolidada deste crescentemente importante campo da economia. Desta forma, navega às cegas, tendendo a se subordinar a padrões e estratégias de grandes players internacionais, colocando em cheque sua soberania em múltiplas dimensões. A ausência de modelos de mensuração e de eleição de dimensões relevantes e indicadores para sua medição contribui para que as políticas públicas tenham dificuldade para determinarem metas claras e mobilizarem os instrumentos adequados para que estas sejam atingidas.

Não por acaso, os planos e estratégias discutidos – digitalização, IA, Internet das coisas, *blockchain*, cibersegurança - se limitam a diretrizes abstratas e não aterrissam em programas e ações concretas, com a identificação de instrumentos de política específicos. A adoção acrítica dos conceitos internacionais e da retórica liberal subjacente contribui para que a tônica nos

documentos de política esteja nos benefícios da adoção de tecnologias, independentemente de suas especificidades técnicas e de que atores e que sistemas de inovação são fortalecidos com a mobilização e desenvolvimento de competências produtivas e tecnológicas.

A ausência de uma conceituação e de critérios de mensuração também contribuem para que inexista um quadro de referência que permita promover o diálogo entre diferentes pastas/ministérios e organizações da administração pública. Muitas das estratégias discutidas acima foram gestadas unicamente dentro do MCTI ou por este ministério em parceria com uma outra organização pública, tais como CGEE e BNDES. Mas efetivamente não se configuram como políticas intersetoriais. Neste sentido, as perspectivas de estímulo ao desenvolvimento de competências no país tendem a se restringir à política tradicional de C&T e à política de ambientes de inovação (PNI) com foco em startups e os tais "ecossistemas empreendedores".

Contudo, especialmente em países periféricos, a lógica de inserção da produção de soluções tecnológicas por startups à demanda potencial de grandes empresas pode contribuir para uma dinâmica desterritorializada. Com o risco de se estabelecerem pouquíssimas conexões efetivas e profundas com as bases de conhecimento e vocações produtivas do território, recursos de apoio à incubação podem estar contribuindo para subsidiar a terceirização da busca tecnológica de grandes corporações. De acordo com Lazonick e Mazzucato (2013) e Mazzucato (2018), isso seria uma nova forma de socialização dos riscos dos investimentos inovativos, com poucos *spillovers* para o território e baixa socialização dos retornos. Trata-se do que Moraes (2020) caracteriza como a tendência à "startupização" inerente ao capitalismo de plataformas.

Contribui para este quadro fragmentado o fato de importantes políticas públicas do atual governo ainda não terem sido divulgadas. A E-digital foi atualizada no final de 2022, antes da posse da atual gestão; as políticas de governo digital e a política industrial e de inovação ainda não saíram do forno. Enquanto ainda são gestadas, já se observa nelas um recorrente traço de colonialismo na importação de conceitos descontextualizados, na medida em que os diversos órgãos da política pública adotam uma concepção acríticas de "missões". Em vez de se construir uma visão própria e adequada do futuro da sociedade e o papel que a economia desempenhará neste cenário, com destaque para a economia de dados, o meio – a missão – se transformam no fim.

A análise empreendida neste projeto sobre diversos país ao redor do globo, destacadamente em Lemos (2024) e Arroio (2024) evidenciam um panorama diversificado de posicionamento dos países em face dos desafios e oportunidades trazidos pela economia de dados. Em diversos países, não há capacitação para o desenvolvimento nacional de sistemas e plataformas, contribuindo para que governos contratem diretamente as *big techs* para a formulação, implementação e gestão de seus dados. Outros países buscam um posicionamento que defenda em diferentes níveis a sua soberania. O Brasil possui amplas competências científicas e tecnológicas e um tecido produtivo diversificado, com competências de ponta em diversas áreas. Portanto, não pode se subordinar a uma dinâmica e padrão de desenvolvimento tecnologicamente e culturalmente subordinado.

Portanto, conforme sublinhado repetidas vezes ao longo desta análise, é necessário um conceito de economia de dados culturalmente e politicamente empoderado e adequado a uma perspectiva nacional de desenvolvimento. Em primeiro lugar, não basta uma conceituação que reconheça

que o fenômeno existe. É preciso que a conceituação apresente uma identificação explícita das implicações deste fenômeno. Neste sentido, ele precisa contemplar, a partir das especificidades da sociedade da economia e da institucionalidade nacional, que implicações, desafios e oportunidades traz para as quatro dimensões da soberania delineados neste estudo:

(i) Segurança nacional e defesa do estado de direito;

(ii) Promoção de uma autonomia econômica em relação a tecnologias estrangeiras e provedores de serviços;

(iii) Promoção de autonomia dos usuários e de autodeterminação individual

(iv) Proteção da identidade e diversidade sociocultural, promovendo a proteção do patrimônio cultural, a diversidade, a valorização dos diversos grupos, comunidades e territórios e a valorização de epistemes próprias

A consideração das especificidades de um país como o Brasil evidencia como é especialmente importante, por exemplo, a consideração deste quarto ponto, que é apenas marginalmente contemplado na literatura advinda dos países centrais. Uma conceituação útil de economia de dados precisa considerar os mecanismos através dos quais diferentes vozes e epistemes são potencializadas ou sufocadas e de que forma isto impacta no desenvolvimento regional e territorial de um país multicultural.

Em segundo lugar, não basta que uma conceituação identifique os processos envolvidos de geração, processamento e análise de dados, entre outros. É preciso que esta contextualize estes processos em uma perspectiva efetivamente sistêmica de um sistema produtivo e inovativo da economia de dados. Tal perspectiva é pré-requisito para que se logre superar um cenário de profusão de missões uniministeriais e que se avance em direção a políticas públicas efetivamente intersetoriais, ancoradas em uma perspectiva sólida de desenvolvimento e no entendimento de como as especificidades do tecido social, econômico e institucional do país estabelecem desafios e também oportunidades para este processo.

Em terceiro lugar, uma conceituação útil precisa traçar um panorama claro – também derivados dos dois pontos anteriores – de que fenômenos devem ser mensurados e que indicadores e métricas devem ser empregadas. Em perspectiva pragmática de atuação de gestores públicos, o sucesso de sua intervenção é determinado de acordo com as métricas anteriormente definidas. Neste sentido, a construção de métricas, indicadores e índices não é neutro, constituindo um processo político e estratégico.

Referências Bibliográficas

AMADEU, S. Lula e a inteligência artificial. Outras palavras, 18 de março de 2024, disponível em: <https://outraspalavras.net/outrasmidias/lula-e-a-inteligencia-artificial/ 2024>, acesso em 01/04/2024.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE – ABES. Mercado Brasileiro de Software: panorama e tendências, 2023. São Paulo: ABES, 2023.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE (ABES). Mercado Brasileiro de Software: panorama e tendências. 1ª. ed. São Paulo: ABES, 2023.

BAILEY, R.; PARSHEERA, S. Data localization in India: paradigms and processes. CSI Transactions on ICT, v. 9, p. 137–150, 2021. https://doi.org/10.1007/s40012-021-00337-4

BARLOW, J. P. Declaração de Independência do Ciberespaço, Davos, Suíça 8 de fevereiro de 1996.

BARRIOS, L. de G. Soberania, Planejamento Estatal e Transformação Digital: análise comparada dos instrumentos jurídicos da União Europeia e do Brasil. Revista Semestral de Direito Econômico, Porto Alegre, v. 2, n. 1, p. e2106, 2023.

BAUMS, A. Digitale Standortpolitik in der Post-Snowden-Welt. In: M. Friedrichsen & P.-J. Bisa (ed.), Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft. p. 223–235, Springer VS, 2016.

BEAN, C. Independent Review of UK Economic Statistics. Londres: LSE, 2016.

BELLI, L. AND GASPAR, W. B. (Eds), The Quest for AI Sovereignty, Transparency and Accountability, Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition. Preliminary version of the outcome report presented at the United Nations Internet Governance Forum (IGF), in Kyoto, Japan, in October 2023.

BMBF. "GAIA-X“: Ein neuer Datenraum für Europa. Bundesministerium für Bildung und Forschung. 2019. Disponível em: <https://www.bmbf.de/de/gaia-x-ein-neuer-datenraum-fuer-europa-9996.html>

BRASIL. Ministro da Ciência, Tecnologia, Inovações e Comunicações. Estratégia Brasileira para a Transformação Digital, 2018. Disponível em: <https://www.gov.br/mcti/pt-br/centraisde-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>.

BRIA, F. Public policies for digital sovereignty. Platform Cooperativism Consortium conference, New York, 2015. https://www.academia.edu/19102224/Public_policies_for_digital_sovereignty

CASSINO, J. F.; SOUZA, J.; SILVEIRA, S. A. (org.). Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Fundação Perseu Abramo, 2021.

CASSIOLATO, J. E.; LASTRES, H. M. M. Sistemas de inovação e desenvolvimento: as implicações de política. São Paulo: São Paulo Perspec., v. 19, n. 1, p. 34-45, 2005.

CASSIOLATO, J. E.; MATOS, M. P.; LASTRES, H. M. M. Innovation Systems and Development. In: Currie-alder, B.; Kanbur, R.; Malone, D. M.; Medhora, R. (Eds.). International Development Ideas, Experience and Prospects. Oxford: Oxford University Press, 2014.

CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS - CGEE. Estratégia Brasileira para a Transformação Digital (E-Digital). Ciclo 2022-2026. Brasília, 2022.

CHENOU, J.-M. From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalisation of internet governance in the 1990s. Globalizations, v. 11, n. 2, p. 205–223, 2014.

CHOHAN, U. W. The Decentralized Autonomous Organization and Governance Issues. Regulation of Financial Institutions eJournal: Social Science Research Network (SSRN). 5 December 2017. Disponível em: http://dx.doi.org/10.2139/ssrn.3082055, acesso em 01/09/2023.

De La Chapelle, B. and L. Porciuncula. We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network, 2021.

DE LA CHAPELLE, B.; PORCIUNCULA, L. We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network, 2021.

DISTRITO. Inteligência Artificial Report. São Paulo: Distrito, janeiro 2021.

FIGUEREDO, C.; MELLO, H. D. Publicidade na era do consumidor digital: como o crescimento das mídias sociais vem interferindo no modo de fazer. Especialização em Marketing Digital e Comércio Eletrônico, da Universidade do Sul de Santa Catarina, Julho, 2017.

FLORIDI ,L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology, v. 33, p. 369–378, 2020.

FLORIDI, L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology, v. 33, p. 369–378, 2020.

GLASZE, G.; DAMMANN, F. Von der "globalen Informationsgesellschaft" zum "Schengenraum für Daten" - Raumkonzepte in der Regierung der "digitalen Transformation" in Deutschland. In: Döbler, Thomas; Pentzold, Christian; Katzenbach, Christian (org.). Räume digitaler Kommunikation, p.159-182, Köln: Herbert von Halem Verlag, 2021.

GOFF, P. Cultural Sovereignty in a Digital Age. In: David Carment, Laura Macdonald, Jeremy Paltiel (ed.) Canada and Great Power Competition, p.191-208, Palgrave Macmillan Cham ,2022.

HILL, J. F. The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders. Lawfare Research Paper Series, v. 2, n. 3, p. 1–41, 2014.

HOFMANN, J. Multi-stakeholderism in Internet governance: Putting a fiction into practice. Journal of Cyber Policy, v. 1, n. 1, p. 29–49, 2016.

HÖPER, L.; SCHULTE, C. Datenbewusstsein im Kontext digitaler Kompetenzen für einen selbstbestimmten Umgang mit datengetriebenen digitalen Artefakten. Gesellschaft für Informatik e.V. (GI) GI. (Hrsg.): INFORMATIK 2021, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021.

IDC, 2022. European DATA Market Study 2021–2023.

KATZ, J. Birth of a Digital Nation. In Wired, 1997. https://www.wired.com/1997/04/netizen-3/.

KLIMBURG, A. The darkening web : the war for cyberspace. Penguin Press, 2017.

LASTRES, H. M. M.; CASSIOLATO, J. E. APLs, conhecimento, desenvolvimento e os desafios da colonialidade do saber. In: Matos, M. P.; Cassiolato, J. E.; Lastres, H. M. M.; Lemos, C.; Szapiro, M. H. S. (orgs.) Arranjos Produtivos Locais: referencial, experiências e políticas em 20 anos da RedeSist. Rio de Janeiro: E-Papers, 2017.

LEE, S. International Reactions to U.S. Cybersecurity Policy: The BRICS Undersea Cable. Henry M. Jackson School of International Studies, Cybersecurity Initiative, January 8, 2016.

MATOS, M. P.; CASSIOLATO, J. E.; LASTRES, H. M. M.; LEMOS, C.; SZAPIRO, M. H. S. (orgs.) Arranjos Produtivos Locais: referencial, experiências e políticas em 20 anos da RedeSist. Rio de Janeiro: E-Papers, 2017.

MAZZUCATO. M.; KATTEL, R.; O'REILLY, T.; ENTSMINGER, J. Reimagining the Platform Economy. Project Syndicate, fevereiro, 2021. Disponível em: <https://www.project-syndicate.org/onpoint/platform-economy-data-generation-and-value-extraction-by-mariana-mazzucato-et-al-2021-02>

PESSANHA, R. M. Capitalismo de plataformas e Aplicação no Brasil e no mundo expõem a superexploração do trabalho. Online, 2020. Disponível em: <http://www.robertomoraes.com.br/2020/06/capitalismo-de-plataformas-e-appficacao.html>.

PESSANHA, R. M. Inovação, financeirização e startups como instrumentos e etapas do capitalismo de plataformas, in: Geografia da Inovação: Território, Redes e Finança, Gomes, M. T., Tunes, R. e Oliveira, F. G. P.433- 468 Rio de Janeiro. Consequência, 2020.

MOVIMENTO BRASIL DIGITAL; PRICE WATERHOUSE COOPERS – PwC. Universo blockchain: guia e estudo sobre o uso da tecnologia no Brasil, 2022.

OLIVEIRA, J. P. Empresas e órgãos públicos podem contratar data centers no exterior. Editorial Empresarial Tecnologia, 17 de março de 2017. Disponível em: https://www.conjur.com.br/2017-mar-17/empresas-orgaos-publicos-podem-contratar-data-centers-exterior/

ONDRÁŠIK, B. Death of the "Free Internet Myth". Masaryk University Journal of Law and Technology, vol. 1, n. 2, p. 75-107, 2007.;

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. Data economy: radical transformation or dystopia?. Frontier Technology Quarterly, janeiro, 2019. Disponível em: <https://www.un.org/development/desa/dpad/publication/frontier-technology-quarterly-january-2019/>

PAZ FILHO, J. S. A evolução da regulamentação dos serviços de internet no Brasil. Cadernos ASLEGIS, n. 38, 2013, p. 47-68, p. 49.

PISTOR, K. Statehood in the digital age. Constellations, v. 27, n. 1, p. 3–18, 2020.

POHLE, J.; THIEL, T. Digital sovereignty. Internet Policy Review, v. 9, n.4, 2020.

POHLE, J.; THIEL, T. Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses. In: I. Borucki & W. J. Schünemann (Eds.), Internet und Staat: Perspektiven auf eine komplizierte Beziehung. p. 57–80, Nomos, 2019.

QUIJANO, A. Colonialidad y modernidad/racionalidad. Perú Indígena (Lima) Vol. 13, n. 29, 1992.

QUIJANO, A. Colonialidade do poder, Eurocentrismo e América Latina. In: A colonialidade do saber: eurocentrismo e ciências sociais. Perspectivas latino-americanas. Buenos Aires, CLACSO, Consejo Latinoamericano de Ciencias Sociales, 2005.

RAYMOND, M., & DENARDIS, L. Multistakeholderism: Anatomy of an inchoate global institution. International Theory. V. 7, n. 3, p. 572–616, 2015.

RICAURTE, P. Data epistemologies, The coloniality of power, and resistance. Television & New Media, 20(4), 350–365, 2019.

SESTINOA, A.; KAHLAWIB, A.; DE MAURO, A. Decoding the data economy: a literature review of its impact on business, society and digital transformation. European Journal of Innovation Management, 2023.

SILVEIRA, S. A. A hipótese do colonialismo de dados e o neoliberalismo. In: Cassino, João Francisco; Souza, Joyce; Silveira, Sérgio Amadeu (org.). Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Fundação Perseu Abramo, 2021.

SOUZA SANTOS; B. Renovar a teoria crítica e reinventar a emancipação social. São Paulo: Boitempo, 2007.

SOUZA SANTOS; B.; MENESES, M. P. (orgs.). Epistemologias do Sul. Coimbra: Almedina, 2009.

SUMMA, H. A. How GAIA-X is paving the way to European data sovereignty. Dotmagazine, Março, 2020. Disponível em: <https://www.dotmagazine.online/issues/cloud-and-orientation/build-your-own-internet-gaia-x>

SZAPIRO, M.; MATOS, M.; CASSIOLATO, J. E.; Sistemas de Inovação e Desenvolvimento. In: RAPINI, M. S.; SILVA, L. A.; ALBUQUERQUE, E. M. (Org.) Economia da Ciência, Tecnologia e Inovação: Fundamentos teóricos e a economia global. Curitiba: Ed. Prismas. cap. 10, p 371- 412, 2017.

TAYLOR, J.; KUKUTAI, T. Indigenous data sovereignty: Toward an agenda. In. Acton, ACT, Australia: Australian National University Press, 2016.

UNCTAD, Digital Economy Report 2021 - Cross-border data flows and development: for whom the data flow, 2021.

ZUBOFF, S. The age of surveillance capitalism: the fight for the human future at the new frontier of power. New York: Public Affairs Books, 2018.