UNIVERSIDADE FEDERAL DO ABC
PROGRAMA DE PÓS-GRADUAÇÃO EM
CIÊNCIAS HUMANAS E SOCIAIS

João Francisco Cassino

SOBERANIA FATIADA: CONTROLE DAS INFRAESTRUTURAS E SUBORDINAÇÃO DA AUTORIDADE PÚBLICA NO MUNDO DIGITAL

São Bernardo do Campo-SP
2025

JOÃO FRANCISCO CASSINO

SOBERANIA FATIADA: CONTROLE DAS INFRAESTRUTURAS E SUBORDINAÇÃO DA AUTORIDADE PÚBLICA NO MUNDO DIGITAL

Tese apresentada ao curso de pós-graduação em Ciências Humanas e Sociais da Universidade Federal do ABC como requisito parcial para obtenção do título de Doutor em Ciências Humanas e Sociais.

Orientador: Prof. Dr. Sérgio Amadeu da Silveira

São Bernardo do Campo-SP

2025

Ficha catalográfica

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Cassino, João Francisco
Soberania Fatiada : Controle das Infraestruturas e Subordinação da Autoridade Pública no Mundo Digital / João Francisco Cassino. — 2025.

190 fls. : il.

Orientação de: Sérgio Amadeu da Silveira

Tese (Doutorado) — Universidade Federal do ABC, Programa de Pós-Graduação em Ciências Humanas e Sociais, São Bernardo do Campo, 2025.

1. Soberania Digital. 2. Soberania de Dados. 3. Políticas Públicas. 4. Gestão Pública. 5. Tecnologias da Informação e da Comuncação. I. Silveira, Sérgio Amadeu da. II. Programa de Pós-Graduação em Ciências Humanas e Sociais, 2025. III. Título.

Declaração de atendimento às observações da banca examinadora

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca examinadora no dia da defesa, sob responsabilidade única do autor e com a anuência do orientador.

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Avenida dos Estados, 5001 - Bairro Santa Terezinha - Santo André - SP
CEP 09210-580 · Fone: (11) 4996-0017

Ata de Defesa de Tese de Doutorado e Folha de Assinaturas

No dia 2 de Junho de 2025 às 14:00, no local: Sala 211 do Bloco Zeta do Campus de São Bernardo do Campo da Universidade Federal do ABC, realizou-se a Defesa da Tese de Doutorado, que constou da apresentação do trabalho intitulado "Soberania Fatiada: Controle das Infraestruturas e Subordinação da Autoridade Pública no Mundo Digital" de autoria do candidato, JOÃO FRANCISCO CASSINO, RA nº 23202010042, discente do Programa de Pós-Graduação em CIÊNCIAS HUMANAS E SOCIAIS da UFABC, sob orientação do Profº SERGIO AMADEU DA SILVEIRA. Concluídos os trabalhos de apresentação e arguição, o candidato foi considerado APROVADO pela Banca Examinadora.

E, para constar, foi lavrada a presente ata e folha de assinaturas assinada pelos membros da Banca.

Dr. SERGIO AMADEU DA SILVEIRA, UFABC
Presidente - Interno ao Programa

Dr. CLAUDIO LUIS DE CAMARGO PENTEADO, UFABC
Membro Titular - Examinador(a) Interno ao Programa

Dr. FLAVIO ROCHA DE OLIVEIRA, UFABC
Membro Titular - Examinador(a) Externo ao Programa

Dr. RODOLFO DA SILVA AVELINO, INSPER
Membro Titular - Examinador(a) Externo à Instituição

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Avenida dos Estados, 5001 - Bairro Santa Terezinha - Santo André - SP
CEP 09210-580 · Fone: (11) 4996-0017

Dra. ROSEMARY SEGURADO, PUC - SP
Membro Titular - Examinador(a) Externo à Instituição

Dra. MARILDA APARECIDA DE MENEZES, UFABC
Membro Suplente - Examinador(a) Interno ao Programa

Dr. RODRIGO TARCHIANI SAVAZONI
Membro Suplente - Examinador(a) Externo à Instituição

Dra. JOYCE ARIANE DE SOUZA MALDONADO
Membro Suplente - Examinador(a) Externo à Instituição

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Avenida dos Estados, 5001 - Bairro Santa Terezinha - Santo André - SP
CEP 09210-580 · Fone: (11) 4996-0017

Folha de Ressalvas

(não incluir esta Folha de Ressalvas na versão final da Tese)

Ressalvas e sugestões da Banca examinadora:

Os membros que participaram de modo remoto foram:

Por sugestão da banca examinadora, o **novo título** passa a ser (em letra de forma e legível):

Indique o **idioma** da dissertação/tese: ☐ **Português** ☐ **Inglês** ☐ **Outro:** _____

a) Novo Título em **Português** (se a dissertação/tese é em português):

b) Novo Título em **Inglês** (preenchimento obrigatório para dissertação/tese em qualquer idioma):

c) Novo Título em **outro idioma**, conforme o idioma indicado acima, se houver:

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

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001

Dedicatória

Dedico este trabalho à minha mamãe, Lionete Cassino, e ao meu papai, João Baptista Cassino (*in memoriam*), que me deram toda a base necessária para que eu chegasse até aqui. Ao meu irmão Juliano, à minha esposa Léia, aos meus sogros, Valéria Coutinho e Irío Ruiz, e ao sobrinho Gustavão.

Agradecimentos

A realização deste doutorado foi uma jornada que teve início em 2017, quando ingressei como aluno especial no mestrado do Programa de Pós-graduação em Ciências Humanas e Sociais da UFABC. Em 2018, formalizei minha entrada no mestrado, e, em 2019, defendi minha dissertação. Também fui aprovado no processo seletivo do doutorado. Em 2020, comecei as disciplinas, mas logo veio a pandemia de COVID-19, que impactou profundamente a vida de todos. Dentro do prazo regulamentar, obtive todos os créditos necessários e concluí a redação desta tese em 2025. Ao longo de todo esse período, três pessoas foram essenciais. Em primeiro lugar, minha esposa, Léia Ruiz, que esteve ao meu lado em todos os momentos, compartilhando ideias, leituras e revisões. Em segundo lugar, meu orientador, Sérgio Amadeu da Silveira, amigo de longa data e que também foi meu professor na graduação. Em terceiro, Edmilson “Pajé” de Novais Silva, que, além de ser um grande amigo, foi meu chefe no trabalho e colaborou de maneira fundamental, permitindo flexibilidade para que eu pudesse cursar as aulas presenciais. Também expresso meu agradecimento especial a Gabriel Boscardim de Moraes, que compartilhou materiais de pesquisa essenciais para a redação desta tese. Agradeço aos colegas do Laboratório de Tecnologias Livres (LabLivre) da UFABC, especialmente Joyce Ariane de Souza Maldonado, Rodolfo Avelino, Mariella Mian, Lia Ribeiro, Débora Machado, Rodrigo Savazoni e Luiz Sérgio Canário. Estendo minha gratidão aos professores Cláudio Luis Camargo Penteado e Flávio Rocha de Oliveira. Agradeço ainda à BB Tecnologia e Serviços, na figura de seu Presidente, Gustavo Pacheco Lustosa, e do Gerente de Gestão de Pessoas, Edison Motta, que me concederam um mês de licença pelo Programa de Educação Continuada (PEC) para escrever esta tese. Reconheço também a contribuição de Alline Barreto, responsável pela elaboração das regras do PEC. Registro meu apreço pelo apoio de Ricardo Bimbo Troccoli. Por fim, expresso minha sincera gratidão à longa lista de amigos e amigas que, de alguma forma, contribuíram para a realização deste trabalho.

Lista de Ilustrações

Figura 1: Oito camadas das infraestruturas do digital.....19
Figura 2: Vista de um eclipse solar de um satélite Starlink em órbita.....53
Figura 3: The Stack – Diagrama de Metahaven.....73
Figura 4: Descrição das camadas TCP/IP e dos SDOs.....75
Figura 5: Camadas do Microsoft Cloud for Sovereignty.....76
Figura 6: Uso anual de água pela Google em The Dalles, em galões.....79
Figura 7: Sistema Interligado Nacional do Operador Nacional do Sistema, 2023…..81
Figura 8: Mapa da Infraestrutura de Conectividade no Brasil, 2025.....84
Figura 9: Startups abertas no Brasil entre 2000 e 2022.....99
Figura 10: Setores mais ativos para investidores de Venture Capital.....100
Figura 11: Infraestrutura Nacional de Dados, 2024.....105
Figura 12: Fontes dos investimentos do PBIA 2024-2028.....109
Figura 13: Distribuição de laboratórios de IA no Brasil.....111
Figura 14: Impressão de tela do Diário Oficial da União.....120
Figura 15: Exemplo de uso de firewall.....122
Figura 16: Provedores de Nuvem do Serpro Multicloud.....134

Lista de Tabelas

Tabela 1: Número de data centers em atividade no Brasil – 2021.....91
Tabela 2: data centers de Cloud Providers, 2021.....92
Tabela 3: Investimentos previstos para o PBIA 2024-2028.....108
Tabela 4: Tipos descritivos de informação, segundo IN nº 5.....115
Tabela 5: Riscos de soberania em contratos e licenças.....148
Tabela 6: Quadro-resumo das Leis dos EUA.....156
Tabela 7: Plataformas gigantes conforme a DSA europeia.....159

Lista de abreviaturas e siglas

ABDI – Agência Brasileira de Desenvolvimento Industrial;
ABES – Associação Brasileira das Empresas de *software*;
ABIN – Agência Brasileira de Inteligência;
ANATEL – Agência Nacional de Telecomunicações;
ANEEL – Agência Nacional de Energia Elétrica;
AWS – Amazon Web Services;
BSI – Bundesamt für Sicherheit in der Informationstechnik (Escritório Federal Alemão de Segurança da Informação);
CALEA – Communications Assistance for Law Enforcement Act (Lei de Auxílio das Comunicações para a aplicação do Direito);
CBD – Catálogo de Bases de Dados, do Governo Federal do Brasil;
CCPA – California Consumer Privacy Act (Lei de Privacidade do Consumidor da Califórnia);
CEITEC – Centro Nacional de Tecnologia Eletrônica Avançada S.A;
CIA – Central Intelligence Agency (Agência Central de Inteligência, dos EUA);
CISA – Cybersecurity Information Sharing Act (Lei de Compartilhamento de Informações de Segurança Cibernética);
CISL – Comitê de Implementação de *software* Livre, do Governo Federal do Brasil;
CNI – Confederação Nacional da Indústria;
DATAPREV – Empresa de Tecnologia e Informações da Previdência;
DATASUS – Departamento de Informática do Sistema Único de Saúde;
DMA – Digital Markets Act (Lei do Mercado Digital);
DSA – Digital Services Act (Lei de Serviços Digitais);
EBIA – Estratégia Brasileira de Inteligência Artificial;
ECPA – Electronic Communications Privacy Act (Lei de Privacidade das Comunicações Eletrônicas);
E-Digital – Estratégia Brasileira para a Transformação Digital;
EUCS – European Union Cloud Certification Scheme (Padrões de segurança cibernética europeia);

FISA – Foreign Intelligence Surveillance Act (Lei de Vigilância de Inteligência Estrangeira);
FNDTC – Fundo Nacional de Desenvolvimento Científico e Tecnológico;
GAFAM – As cinco maiores *Big Techs* dos EUA: Google/Alphabet, Apple, Facebook/Meta, Amazon e Microsoft;
GDC – Google Distributed Cloud;
GPDR – European Union General Data Protection Regulation (Regulamento Geral de Proteção de Dados);
GSI/PR – Gabinete de Segurança Institucional da Presidência da República;
IBGE – Instituto Brasileiro de Geografia e Estatística;
IEA – Agência Internacional de Energia;
IND – Infraestrutura Nacional de Dados;
INEP – Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira;
INPI – Instituto Nacional de Propriedade Intelectual;
IPEA – Instituto de Pesquisa Econômica Aplicada;
ITU – International Telecommunication Union;
LabLivre – Laboratório de Tecnologias Livres da UFABC;
LGPD – Lei Geral de Proteção de Dados Pessoais;
MCTI – Ministério da Ciência, Tecnologia e Inovação;
MDIC – Ministério do Desenvolvimento, Indústria, Comércio e Serviços;
MGI – Ministério da Gestão e da Inovação em Serviços Públicos;
MLAT – Mutual Legal Assistance Treaty (Tratado de Assistência Legal Mútua);
NIB – Nova Indústria Brasil;
NSA – National Security Agency (Agência de Segurança Nacional, dos EUA);
OCI – Oracle Cloud Infrastructure;
PBIA – Plano Brasileiro de Inteligência Artificial;
PNSI – Política Nacional de Segurança da Informação;
SCA – Stored Communications Act (Lei de Comunicações Armazenadas);
SERPRO – Serviço Federal de Processamento de Dados;
SGD – Secretaria de Governo Digital;
TSE – Tribunal Superior Eleitoral;
UFABC – Universidade Federal do ABC.

RESUMO

A presente Tese de Doutorado parte da necessidade do Estado brasileiro intensificar o uso de tecnologias digitais no mundo contemporâneo. No entanto, para além das inúmeras vantagens que essas tecnologias trazem, há efeitos adversos, como o risco de fuga de dados sensíveis para fora do controle estatal e a dependência da administração pública das grandes empresas do setor de Tecnologias da Informação e da Comunicação. Para compreender o problema, esta pesquisa realizou uma detalhada revisão bibliográfica sobre as principais teorias que abordam esta realidade. Também retoma a discussão sobre o que é o conceito de soberania e as alterações que vem sofrido nas últimas décadas. A soberania passa a ser fatiada, com o Estado tornando-se refém de infraestruturas controladas por empresas privadas ou privatizadas, sendo a maior parte delas multinacionais estrangeiras. As soluções tecnológicas que o Estado brasileiro está adotando para superar as condições de perda de *soberania digital* e de *soberania de dados* são insuficientes. Os produtos e serviços dos modelos de “nuvens soberanas” em implantação mantêm o Brasil em uma condição bastante frágil em relação ao poder das *Big Techs*. A pesquisa analisa contratos, licenças de uso e legislações do Brasil, EUA e União Europeia para comprovar como a atual situação não melhora a posição brasileira, que segue como vítima de um novo tipo de colonialismo na era digital.

PALAVRAS-CHAVE:

Soberania Digital; *Soberania de Dados*; Tecnologias da Informação e da Comunicação; Políticas Públicas; Gestão Pública.

ABSTRACT

This Doctoral Thesis is based on the need for the Brazilian State to intensify the use of digital technologies in the contemporary world. However, in addition to the numerous advantages that these technologies bring, there are adverse effects, such as the risk of sensitive data leaking out of state control and the dependence of the public administration on large companies in the Information and Communication Technologies sector. To understand the problem, this research carried out a detailed bibliographic review on the main theories that address this reality. It also resumes the discussion on what the concept of sovereignty is and the changes it has undergone in recent decades. Sovereignty is becoming sliced, with the State becoming hostage to infrastructures controlled by private or privatized companies, most of which are foreign multinationals. The technological solutions that the Brazilian State is adopting to overcome the conditions of loss of digital sovereignty and data sovereignty are insufficient. The products and services of the "sovereign cloud" models being implemented keep Brazil in a very fragile condition in relation to the power of Big Techs. The research analyzes contracts, usage licenses and legislation from Brazil, the USA and the European Union to prove how the current situation does not improve Brazil's position, which continues to be a victim of a new type of colonialism in the digital age.

KEYWORDS:

Digital Sovereignty; Data Sovereignty; Information and Communication Technologies; Public Policies; Public Management.

RESUMEN

Esta Tesis Doctoral se fundamenta en la necesidad de que el Estado brasileño intensifique el uso de las tecnologías digitales en el mundo contemporáneo. Sin embargo, además de las numerosas ventajas que estas tecnologías aportan, existen efectos adversos, como el riesgo de fuga de datos sensibles fuera del control estatal y la dependencia de la administración pública de las grandes empresas del sector de las Tecnologías de la Información y la Comunicación. Para comprender la problemática, esta investigación realizó una revisión bibliográfica detallada sobre las principales teorías que abordan esta realidad. También retoma la discusión sobre qué es el concepto de soberanía y los cambios que ha sufrido en las últimas décadas. La soberanía está ahora dividida y el Estado se ha convertido en rehén de infraestructuras controladas por empresas privadas o privatizadas, muchas de ellas multinacionales extranjeras. Las soluciones tecnológicas que el Estado brasileño está adoptando para superar las condiciones de pérdida de soberania digital y de soberanía de datos son insuficientes. Los productos y servicios de los modelos de "nube soberana" que se están implementando mantienen a Brasil en una condición muy frágil en relación al poder de las Big Techs. La investigación analiza contratos, licencias de uso y legislación de Brasil, EE.UU. y la Unión Europea para comprobar cómo la situación actual no mejora la posición de Brasil, que sigue siendo víctima de un nuevo tipo de colonialismo en la era digital.

PALAVRAS CLAVE:

soberania digital; Soberanía de datos; Tecnologías de la Información y la Comunicación; Políticas Públicas; Gestión Pública.

Sumário

INTRODUÇÃO....16

Ficha Técnica....21
1. Problema de pesquisa....21
2. Hipótese....21
3. Objetivos....22
3.1. Objetivo principal....22
3.2. Objetivos secundários....22
4. Metodologia....23

CAPÍTULO 1: DAS ANÁLISES DO MUNDO DIGITAL....24

1.1. Tecnofeudalismo....24
1.2. Um novo colonialismo?....28
1.2.1. Colonialismo Digital....28
1.2.2. Colonialismo de Dados....31
1.2.3. Da violência material no colonialismo histórico....34
1.3. Ainda o mau e velho capitalismo....36
1.3.1. Capitalismo Digital....37
1.3.2. Capitalismo Cognitivo....38
1.3.3. Capitalismo de Vigilância....39
1.3.4. Capitalismo de Plataforma....41
1.3.5. Dataficação, dataísmo e vigilância de dados....43

CAPÍTULO 2: DA SOBERANIA....45

2.1. A Guerra dos Trinta Anos e a Soberania Estatal como a conhecemos....47
2.2. Dinâmica geopolítica global em 2025....52
2.3. Soberania digital e soberania de dados....54
2.4. Faça o que eu digo, não faça o que eu faço....59
2.5. Quebrando todas as regras....61
2.6. Soberania à venda … mas quem está comprando?....64

CAPÍTULO 3: DO FATIAMENTO DA SOBERANIA....69

3.1. Subdivisões na camada de Nuvem....71
3.2. Infraestruturas do digital....73
3.2.1. Energia elétrica....74
3.2.2. Telecomunicações....80
3.2.3. Hardwares e equipamentos....85
3.2.4. Data Centers....87
3.2.5. Softwares básicos....91

3.2.6. Desenvolvimento de sistemas.....94
3.2.7. Bases de dados.....98
3.2.8. Inteligência Artificial.....103

CAPÍTULO 4: A “NUVEM SOBERANA” DO BRASIL.....108

4.1. Soberania como oportunidade de negócios.....113
4.2. A “Nuvem Soberana” do Serpro.....114
4.3. Entrevista com o Presidente do Serpro sobre a Nuvem Soberana.....122

CAPÍTULO 5: REGRAS PARA OS EXPORTADORES DE DADOS.....129

5.1. Contrato da Amazon com o Serpro.....131
5.2. Contrato da Microsoft Azure com o Serpro.....134
5.3. Contrato da Huawei com o Serpro.....137
5.4. Contrato da IBM com o Serpro.....138
5.5. Contrato da Oracle com o Serpro.....139
5.6. Termos específicos de serviço do Google Distributed Cloud air-gapped.....139
5.7. Quadro-resumo.....145

CAPÍTULO 6: DISPOSITIVOS DA LEGISLAÇÃO DOS EUA.....146

6.1. FISA – Foreign Intelligence Surveillance Act (1978).....146
6.2. CALEA – Communications Assistance for Law Enforcement Act (1994).....148
6.3. Patriot Act (2001) e Freedom Act (2015).....150
6.4. Cloud Act (2018).....151
6.5. Outros dispositivos legais dos EUA.....152
6.6. Quadro-resumo.....153

CAPÍTULO 7: PROPOSIÇÕES PARA FORTALECER A SOBERANIA DIGITAL.....154

7.1. Europa contra as Big Techs.....155
7.2. A Iniciativa EuroStack.....157
7.3. Soberania e digitalização democrática na Europa.....159
7.4. Comuns digitais e a Infraestrutura Digital Pública Europeia.....160
7.5. Propostas para o Brasil.....161
7.6. Novas leis para o Brasil.....162
7.7. Propostas para cidades.....162

CONCLUSÃO.....165

REFERÊNCIAS BIBLIOGRÁFICAS.....167

a) Bibliografia Acadêmica.....167
b) Estudos, Fontes Primárias e Oficiais.....172
c) Publicações de Veículos de Imprensa e Portais de Internet.....180

INTRODUÇÃO

A redução da soberania dos estados nacionais frente a intensificação das tecnologias digitais é um problema que afeta todas as nações. Se por um lado a transformação informacional garante muitos benefícios, como uma maior eficiência, potencial redução de procedimentos da burocracia estatal e mais possibilidades de oferta digital de serviços públicos *online,* por outro há a forte dependência dos fornecedores que controlam as tecnologias e graves riscos de fuga de dados estatais sensíveis, como do funcionalismo público, das forças militares, policiais, de inteligência e da população como um todo.

Como proteger a soberania nacional em um mundo digital e conectado é uma pergunta que fazem os governantes preocupados com esta realidade e, portanto, torna-se um problema de pesquisa. A questão não é exatamente nova, tendo sido objeto de análise pelo menos desde os anos 1990, quando a Internet começou a se popularizar. Mesmo assim, surgem novos desafios, como, neste momento, o crescimento do uso de Computação em Nuvem e de Inteligência Artificial, o que gera novos benefícios e também novos riscos.

Há análises de todos os tipos, as que reproduzem os discursos das consultorias de mercado e das agências de *marketing*, as otimistas, as pessimistas, as utópicas e as distópicas. Há as que creem na liberdade irrestrita do mercado, as que defendem que o aperfeiçoamento das leis e a criação de um melhor arcabouço jurídico sejam suficientes para a resolução de todas os problemas, as que buscam acelerar os processos capitalistas e tecnológicos para forçar mudanças sociais, dentre outras.

Agências governamentais e empresas estatais, devido às suas próprias atribuições legais e características, teriam de ser a vanguarda da defesa da *soberania digital*, mas em muitos casos compram os discursos do mercado e adotam os serviços e produtos como uma solução mágica para o setor público no mundo conectado, legitimando suas ações com argumentos típicos de neoliberalismo, de maior velocidade, de inovação e de eficiência.

O enfrentamento à perda de soberania no mundo digital não pode ser feito de uma única maneira. Não adianta simplesmente comprar um pacote de produto de

nuvem soberana e implantá-lo por meio de uma consultoria. Precisa-se agir de uma maneira holística, sobre várias camadas, recuperando-se pedaço por pedaço de uma soberania fatiada. Para tanto, o estado nacional verdadeiramente preocupado com a *soberania digital* deve ter um olhar amplo, considerando a sua capacidade de regulação e de intervenção sobre as oito *infraestruturas do digital*, a saber: 1) energia elétrica; 2) telecomunicações; 3) *hardwares* e equipamentos; 4) *data centers*; 5) desenvolvimento de *softwares* básicos; 6) desenvolvimento de *softwares* e aplicativos; 7) guarda e proteção de bases de dados; e 8) inteligência artificial.

Figura 1 – Oito camadas das infraestruturas do digital

Fonte: elaborado pelo autor (CASSINO, 2025)

Sobre essa ótica, nenhum país será completamente soberano, uma vez que há interdependências em escala global para funcionamento de cada um dessas camadas de infraestrutura. Mas a soberania tecnológica se dá em níveis, com os EUA sendo soberanos no domínio estratégico dos semicondutores aos bancos de dados, tendo capacidade de intervenção superior à de todas as outras nações.

Cada uma das *infraestruturas do digital* é composta por uma rede complexa de atores, por uma grande variedade de empresas, de vários tipos e de tamanhos, localizadas em vários países, que participam de cadeias produtivas integradas, cujos produtos finais podem passar por várias etapas até que estejam prontos para comercialização. Há questões envolvidas relativas à legislação, à regulamentação, à propriedade intelectual e à propriedade industrial. Há ações de organismos internacionais, de governos nacionais e de poderes políticos locais. Há a dinâmica do mercado, o comportamento dos clientes e a satisfação dos usuários dos produtos e dos serviços ofertados. É preciso enxergar as infraestruturas do digital como um ordenamento horizontal, difuso e distribuído, que se espalha por todo o planeta, cuja presença é territorialmente mais densa em alguns locais e menos densa em outros.

A publicidade desempenha um papel muito importante no mundo digital. Utilizando-se de modernos mecanismos algorítmicos, ela se beneficia da captura, armazenamento e processamento de dados pessoais para oferecer produtos comerciais e conteúdos ideológicos de maneira microssegmentada, modulando o comportamento dos indivíduos. Esse modelo de negócios é essencial para algumas das maiores empresas do setor, tais como Google e Facebook/Meta, cuja venda de anúncios é uma parte significativa de suas receitas.

O *marketing* também é usado para comercializar as inovações tecnológicas. Chegam acompanhadas de peças publicitárias sofisticadas, que prometem soluções extraordinárias aos clientes. No discurso da propaganda, tudo parece perfeito. Criam-se diagramas e metodologias impressionantes para persuadir os compradores a aderirem ao solucionismo tecnológico imposto pelas corporações, que, muitas vezes, primeiro desenvolvem o que desejam vender e só depois buscam, na prática, formas de aplicá-lo à vida cotidiana. Surgem termos atrativos, meramente publicitários, que passam a circular como verdades incontestáveis. Um exemplo é o conceito de *transformação digital*, que nada mais é do que uma expressão guarda-chuva usada para agrupar produtos e serviços de TI sem qualquer relação entre si (SILVEIRA, 2024, p. 11-25).

A *computação em nuvem* é mais uma marca criada como estratégia de *marketing*. Ela serve para designar o processamento e o armazenamento de dados em *data centers*, quando o contratante quase sempre desconhece a localização de

seus dados e tem pouca ou nenhuma ingerência sobre seu uso. *Cidades inteligentes* (*Smart Cities*) é outro termo da moda, empregado para embalar soluções e vendê-las a municípios e governos locais, oferecendo redes de sensores conectados por *softwares* que possibilitam algum nível de automação e captura de dados.

Todos os anos, consultorias de mercado e agências de publicidade apresentam novidades. Elas realizam belas apresentações sobre as supostas tendências do futuro, que, na realidade, não passam de um cardápio de produtos e serviços que precisam ser vendidos para garantir bons lucros ao final do próximo trimestre fiscal. A propaganda oculta deliberadamente os riscos da dependência de governos e consumidores em relação às soluções tecnológicas. Pelo contrário, nos planejamentos comerciais, são desenvolvidas técnicas para fidelizar (ou aprisionar) os clientes, dificultando ao máximo sua decisão de abandonar um produto e migrar para outro.

Um exemplo claro disso ocorre quando uma empresa decide mover suas aplicações para um serviço de nuvem. A adesão é extremamente simples, com a maioria dos procedimentos podendo ser realizados por profissionais com pouca experiência. No entanto, sair daquele fornecedor e migrar para um concorrente se transforma em um verdadeiro pesadelo gerencial. As interfaces de administração dos serviços em nuvem são projetadas para facilitar a adesão, mas tornar a saída significativamente mais difícil, criando barreiras que desestimulam a migração dos clientes.

Quem controla as infraestruturas e os sistemas também determina os rumos do mundo digital. O problema é que essas infraestruturas são, em sua maioria, dominadas por oligopólios privados, eliminando qualquer possibilidade de sustentação do discurso liberal de que a concorrência de mercado resolverá todos os problemas. A única forma de enfrentar o poder avassalador das *Big Techs* é por meio da ação estatal. No entanto, poucos países possuem força comparável à das maiores corporações de tecnologia e, ao mesmo tempo, não podem simplesmente deixar de se atualizar tecnologicamente, sob risco de obsolescência funcional e administrativa.

De acordo com a 22ª edição anual do Global 2000 (MURPHY; SCHIFRIN, 2024), levantamento realizado pela revista norte-americana Forbes, três das dez

maiores empresas do mundo em 2024 são gigantes da tecnologia da informação. A Amazon ocupa a 6ª posição, com US$ 590,7 bilhões em vendas no ano e um valor de mercado de US$ 1,9 trilhão. Em 8º lugar está a Microsoft, com vendas de US$ 236,5 bilhões e um valor de mercado de US$ 3,1 trilhões. Já na 10ª posição aparece a Alphabet, controladora do Google, com vendas de US$ 317,9 bilhões e um valor de mercado de US$ 2,1 trilhões.

Comparativamente, a Alemanha, terceira maior economia do mundo em 2023, registrou um Produto Interno Bruto (PIB) de US$ 4,4 trilhões. O Reino Unido, na sexta posição, teve um PIB de US$ 3,3 trilhões (MIATO, 2025). Se a Microsoft fosse um país, ocuparia a sétima colocação, considerando seu valor de mercado. Os PIBs da França, Itália e Brasil, que aparecem logo em seguida na lista, foram de US$ 3 trilhões, US$ 2,18 trilhões e US$ 2,17 trilhões, respectivamente. Países menores possuem PIBs que representam apenas uma fração do valor das grandes corporações. O Uruguai, por exemplo, registrou em 2023 um PIB de apenas US$ 77,2 bilhões, o que equivale a cerca de 4% do valor de mercado da Amazon.

A forma adotada para a construção deste trabalho passa primeiramente pela revisão bibliográfica, observando definições que ocupam o centro do debate acadêmico no que se refere ao tema da *soberania digital* (ou da falta dela). São vários os termos utilizados para descrever esta realidade: colonialismo digital, colonialismo de dados, tecnofeudalismo, capitalismo de vigilância, capitalismo de plataforma, capitalismo cognitivo, dentre outros. Buscaremos entender e examinar essas teorias no capítulo 1.

Em segundo lugar, no capítulo 2, ainda na revisão bibliográfica, será debatido com mais profundidade o conceito clássico de soberania nacional, evoluindo para o entendimento sobre o que é *soberania digital* e *soberania de dados*.

No capítulo 3, veremos o fatiamento da soberania digital e de dados em camadas, em especial, nas *infraestruturas do digital*. Observaremos o status atual de cada uma das infraestruturas no Brasil atualmente.

No capítulo 4, mostraremos como as *Big Techs* transformaram a soberania em um modelo de negócios rentável e como o Estado brasileiro, principalmente por

meio de sua estatal Serpro, tem reduzido sua *soberania digital*, apesar de, paradoxalmente, adotar um discurso de *soberania de dados*.

Os capítulos 5 e 6 complementam o capítulo 4. No quinto, ocorre a análise dos contratos do Serpro com seis das maiores *Big Techs*, sendo cinco norte-americanas e uma chinesa. No sexto, como as leis dos Estados Unidos obrigam suas empresas a criar mecanismos para facilitar a vigilância de sistemas digitais.

Por fim, o capítulo 7 apresenta reflexões sobre o que está sendo feito na União Europeia e o que o Brasil poderia fazer para melhorar sua condição de dependência no mundo digital.

Ficha Técnica

1. Problema de pesquisa:

Como enfrentar a perda de soberania decorrente da intensificação do uso de tecnologias digitais? Os produtos e serviços ofertados pelas gigantes de tecnologia que prometem garantir a *soberania digital* e *soberania de dados* são confiáveis, eles realmente impedem a captura de dados estratégicos nacionais por terceiros?

2. Hipótese:

As soluções tecnológicas que o Estado brasileiro está adotando para superar as condições de perda de *soberania digital* e de *soberania de dados* são insuficientes. Os produtos e serviços dos modelos de “nuvens soberanas” em implantação tornam o Estado refém de fornecedores estrangeiros e vulnerável à perda de dados.

3. Objetivos:

3.1. Objetivo principal:

Comprovar que as promessas de *soberania digital* por meio de produtos e serviços das *Big Techs* apresentam sérias limitações para estados nacionais que buscam sua verdadeira autonomia tecnológica.

3.2. Objetivos secundários:

- Apresentar as principais teorias que analisam a realidade atual geopolítica frente ao poder das grandes empresas de Tecnologias da Informação e da Comunicação;
- Discutir o conceito de soberania e como ele vem sendo alterado nas últimas décadas, assim como entender os conceitos de *soberania digital* e de *soberania de dados*;
- Debater o fatiamento da soberania e de sua distribuição por meio de avaliação sobre quem controla as infraestruturas do digital (energia elétrica, telecomunicações, *hardwares*, *data centers*, *softwares*, aplicativos, bases de dados e Inteligência Artificial);
- Analisar a política de nuvem soberana que o Governo Federal do Brasil vem implementando, com um olhar mais detalhado para o caso do Serpro;
- Analisar as principais cláusulas dos contratos de parceria do Serpro com as *Big Techs* para fornecimento de serviços *multicloud* para o Governo Federal;
- Debater os dispositivos da legislação norte-americana que lhe dá respaldo legal para cobrar o fornecimento de dados pelas *Big Techs* para os serviços de Inteligência dos EUA;
- Analisar o que a União Europeia está planejando fazer para reduzir sua condição de dependência das *Big Techs* chinesas e norte-americanas;
- Oferecer recomendações de como o Brasil pode reduzir sua situação de dependência digital.

4. Metodologia:

- Revisão bibliográfica;
- Pesquisa em matérias de jornais, revistas e portais *web* em busca de fatos que ilustrem e comprovem a hipótese;
- Pesquisa em leis, normativos e outras regulamentações, principalmente do Brasil e dos Estados Unidos.
- Pesquisa empírica a partir da realidade do Estado brasileiro, com olhar para a situação atual das infraestruturas do digital no Brasil;
- Análise da implementação de produtos e serviços de *soberania digital* no Estado brasileiro.

CAPÍTULO 1
DAS ANÁLISES DO MUNDO DIGITAL

A perda da soberania nacional no mundo digital é objeto de estudo de diversos autores e autoras ao redor do globo, como Yanis Varoufakis, Cédric Durand, Evgeny Morozov, Michael Kwet, Nick Couldry, Ulises Mejias, Daniel Schiller, Yann Moulier-Boutang, Shoshana Zuboff, Nick Srnicek, José Van Dijck e Sérgio Amadeu da Silveira.

Neste capítulo, serão apresentados pontos relevantes da obra de cada um deles para a compreensão da temática da *soberania digital*. Cada autor coloca seu foco em alguns aspectos deste problema que marca nosso tempo. A depender de cada olhar, obtemos percepções diferentes e nomenclaturas diversas, que, juntas, ajudam a formar um panorama amplo e complexo.

1.1. Tecnofeudalismo

O poder de definir os rumos das tecnologias, o poder econômico e as influências sociais e políticas das *Big Techs* levam alguns autores a propor o termo *tecnofeudalismo* para descrever a nossa realidade. O feudalismo histórico ocorreu entre os séculos V e XV, como consequência da desintegração do Império Romano, resultando em uma nova organização social, política e econômica na Europa.

Os feudos eram grandes propriedades rurais controladas pela nobreza, composta pelos proprietários das terras, que também exerciam a defesa militar dos territórios. O plantio e outros serviços essenciais ficavam sob a responsabilidade dos servos, que recebiam proteção da nobreza e o direito de cultivar parcelas de terra para sua subsistência. Havia ainda uma forte influência do clero, tornando o cristianismo um elemento de unidade nos espaços feudais europeus.

Yanis Varoufakis, economista e ex-ministro das Finanças da Grécia, acredita que o mundo está passando por uma transição do capitalismo para o tecnofeudalismo. Ele explica que, assim como o capitalismo surgiu a partir do antigo feudalismo, hoje temos um novo modelo econômico denominado tecnofeudalismo que pode substituir ou transformar drasticamente o atual modelo capitalista. Um dos

sinais desse processo é o evidente deslocamento entre a economia real e o que ocorre no mercado financeiro (VAROUFAKIS, 2024).

No passado, o capitalismo passou por transformações extremas. Varoufakis considera que uma delas foi a Segunda Revolução Industrial, quando o oligopólio substituiu o “disfarce competitivo” e surgiram os megabancos, essenciais para financiar as grandes corporações. Nos anos 1970, com a crise do sistema de Bretton Woods (criado para reorganizar a economia global no pós-Segunda Guerra Mundial), os EUA se tornaram o principal fornecedor mundial de demanda agregada e absorvedor de exportações líquidas de países como Alemanha, Japão e, posteriormente, China. Aos poucos, regulamentações e restrições que organizavam o capitalismo em sua fase anterior foram sendo eliminadas, transformando o capitalismo oligopolista em capitalismo financeiro. No entanto, em ambas as etapas, o capitalismo permaneceu impulsionado pelo “lucro privado” e pelos “aluguéis extraídos de algum mercado”.

A crise de 2008 foi desencadeada pelo estouro da bolha imobiliária nos Estados Unidos, provocada pela escalada dos preços dos imóveis, tornando-os incompatíveis com a renda da população. Considerada a pior crise financeira desde a Grande Depressão de 1929, ela levou ao colapso de algumas das mais tradicionais instituições financeiras. Varoufakis explica que isso forçou os bancos centrais do G7 (grupo que reúne as sete maiores economias do mundo) a utilizar sua capacidade de imprimir dinheiro para reconstruir as finanças globais, tornando a economia mundial dependente dessa forma contínua de geração monetária. O principal motor passou a ser a emissão de dinheiro pelos bancos centrais, e não mais o lucro privado.

Paralelamente, surgiam as plataformas digitais, como Facebook e Amazon, que, segundo Varoufakis, *“não operam mais como empresas oligopolísticas, mas sim como feudos ou propriedades privadas”*. Essas corporações se beneficiam da produção gratuita de capital social. Os conteúdos que alimentam as plataformas são gerados pelos próprios usuários, seja ao publicar algo em uma rede social ou ao utilizar serviços como o Google Maps enquanto dirigem.

O ponto central da visão de Varoufakis é que os setores capitalistas tradicionais não desapareceram, mas se tornaram vassalos das plataformas. Em

uma entrevista publicada em fevereiro de 2023, o ex-ministro grego argumenta que o capitalismo evoluiu para o que ele chama de *capital em nuvem*, marcando o fim do capitalismo tradicional (VAROUFAKIS, 2023).

O *capital em nuvem* criou *feudos digitais*, nos quais todos (proletários, trabalhadores precarizados, burgueses e capitalistas vassalos) produzem mais-valia para as plataformas. Trata-se de um modelo semelhante ao de aluguéis, mas configurado como um *aluguel em nuvem*. Além disso, o dinheiro emitido pelos bancos centrais é o que possibilitou e continua sustentando a evolução do *capital em nuvem*. Em um trecho da entrevista, Varoufakis afirma que:

> *"Se o capitalismo é baseado no mercado e orientado para o lucro, bem, então isso não é mais capitalismo, porque não é baseado no mercado. Ele é baseado em plataformas digitais que estão mais próximas de feudos tecnológicos ou feudos em nuvem, e são impulsionadas por duas formas de liquidez. Um é o aluguel em nuvem, que é o oposto do lucro, e o outro é o dinheiro do banco central, que financiou a construção de capital em nuvem. E isso não é capitalismo."* (VAROUFAKIS, 2024)

Outro pesquisador que também trabalha com o conceito de tecnofeudalismo é Cédric Durand, autor de *Tecnofeudalismo: Crítica de la economía digital* (2021a). No livro, há um capítulo inteiramente dedicado à questão do rentismo de bens intangíveis, destacando que, enquanto terras e bens físicos são elementos tangíveis, a Internet, os *softwares* e os aplicativos são intangíveis. A diferença fundamental entre esses dois tipos de bens é que os tangíveis são escassos e limitados, enquanto os intangíveis podem ser reproduzidos virtualmente de forma infinita. Essa é a razão pela qual, desde as últimas décadas do século XX, a propriedade intelectual tem ganhado cada vez mais importância para os detentores do capital. Para isso, torna-se necessário um monopólio legal sobre conhecimentos, já que esses não estão vinculados a um espaço geolocalizado. O rentismo de bens intangíveis fundamenta-se na capacidade de reprodução extensível desses ativos, que, após um investimento inicial, podem ser replicados com custos marginais.

Cédric Durand também alerta para outro tipo de força decorrente da monopolização intelectual, o que ele chama de "renda de inovação dinâmica". Trata-se de um mecanismo em que, quanto mais integradas e ativas estão as cadeias, mais dados são gerados, armazenados e centralizados, formando grandes massas

de informação que conferem um poder informativo incomparável a quem os detém. Essa dinâmica contribui para a eliminação da concorrência no livre mercado, impondo uma concentração monopolista global e nos inserindo em um *capitalismo feudal*, ou *tecnofeudalismo*. Nele, a vida econômica praticamente deixa de existir fora do domínio das corporações. Quanto mais utilizamos um serviço digital, mais imprescindível ele se torna — e mais dependentes dele ficamos. As empresas capturam mais dados, mais espaços digitais e, consequentemente, ampliam suas fontes de informação. É a lógica da predação feudal sobre as terras atualizada para o digital (DURAND, 2021b).

Em seu ensaio *Crítica da Razão Tecnofeudal* (2022), Evgeny Morozov argumenta que o período pelo qual estamos passando ainda é profundamente capitalista. Pior ainda, o fim do capitalismo pode não significar uma migração para algo melhor, como muitos sonhavam. As distopias se apresentam como possibilidades reais de futuro, fomentando as visões de um novo feudalismo.

Para além de Cédric Durand e Yanis Varoufakis, o artigo de Morozov nos apresenta outros autores, incluindo alguns mais à direita, como Joel Kotkin, Glen Weyl, Eric Posner e Curtis Yarvin, e outros mais à esquerda, como Mariana Mazzucato, Jodi Dean, Robert Kuttner, Wolfgang Streeck, Michael Hudson e Robert Brenner. No entanto, nesta tese de doutorado, não nos aprofundaremos nas outras variações do termo *tecnofeudalismo*, como *neofeudalismo*, *feudalismo digital* ou *feudalismo da informação*, elaborados pelos autores supracitados.

A questão do rentismo digital é um tema recorrente entre esses diversos autores e constitui a base da defesa desse novo feudalismo. As *Big Techs* são rentistas, pois não contribuem diretamente para o processo produtivo real. No entanto, para Morozov, nas diversas adaptações que o capitalismo sofreu ao longo de sua história, a dissociação entre a produção industrial e outras formas de acumulação não é uma novidade. Ele nos remete ao conceito de *despossessão*, idealizado por Harvey, segundo o qual as instituições financeiras atuam sobre os estados nacionais para direcionar a si próprias os recursos públicos. Também nos recorda de Lenin, que se referia à *lógica do parasitismo* para explicar pagamentos de juros, dividendos e taxas de administração.

Morozov ainda faz um alerta: o uso do termo *tecnofeudalismo* (ou suas variantes) pode beneficiar a reputação do capitalismo, pois a perspectiva de uma mudança para algo pior poderia fazer com que a manutenção do sistema atual pareça a opção mais desejável.

1.2. Um novo colonialismo?

Se a ideia de um novo feudalismo não for adequada, como defende Morozov, que tal analisarmos o cenário da sociedade atual, marcado pela ascensão das *Big Techs*, como uma nova forma de colonialismo? Essa é a perspectiva de outros autores, como Michael Kwet, Nick Couldry e Ulises A. Mejias.

1.2.1. Colonialismo Digital

Michael Kwet, em seu artigo *Digital Colonialism: The Evolution of American Empire* (2021), define o colonialismo digital como o uso da tecnologia para a dominação social, política e econômica de outra nação ou território. No colonialismo clássico, os europeus tomaram terras, colonizaram-nas e instalaram portos, ferrovias, bases militares e formas de exploração de matérias-primas e trabalho. Os produtos primários eram então enviados para as metrópoles, onde eram transformados em bens manufaturados.

O colonialismo depende do controle territorial, infraestrutural, da extração de trabalho e conhecimento, bem como da exploração de *commodities*. O processo de exploração evoluiu ao longo dos séculos com o surgimento de novas tecnologias, desde o telégrafo no século XIX até as redes transoceânicas de cabos de fibra ótica que, no século XXI, possibilitam o tráfego de informações.

No mundo digital, pouquíssimas empresas têm capacidade de realizar a captura massiva de dados, armazená-los em vastas fazendas de servidores em nuvem, processá-los e utilizá-los para fins comerciais, de propaganda, políticos e militares. As plataformas digitais e os centros de espionagem, como a CIA e a NSA, são os panópticos da era moderna. Os dados tornaram-se a matéria-prima dos serviços de inteligência.

O poder tecnológico está concentrado em algumas empresas norte-americanas, como Meta/Facebook, Alphabet/Google, Amazon, Microsoft e Apple. As *Big Techs* chinesas, como Baidu, Alibaba, Tencent e Xiaomi, ainda muito localizadas no mercado doméstico e na região próxima à China, começam agora a ganhar relevância global. O restante do mundo permanece em posição secundária, inclusive a Europa, que enfrenta dificuldades para superar as barreiras de entrada nesses segmentos de mercado.

A exploração do trabalho humano no *colonialismo digital* também é uma questão central para Michael Kwet. De um lado, existem exércitos corporativos compostos por uma elite de programadores e engenheiros, cujos salários podem ultrapassar os US$ 250 mil por ano. Por outro, há trabalhadores que são superexplorados e recebem salários miseráveis, seja na extração de minérios essenciais para a produção de *hardware*, na moderação de conteúdos perturbadores e violentos nas redes sociais ou no entediante trabalho de treinamento manual de sistemas de Inteligência Artificial.

Em uma visão geral, Kwet define o colonialismo digital como um meio de perpetuar a divisão desigual do trabalho, no qual potências dominantes utilizam a propriedade das infraestruturas digitais, o conhecimento técnico e o controle sobre os meios de computação para manter o Sul global em uma situação permanente de dependência. Agora, a divisão desigual do trabalho teria evoluído. A manufatura industrial perdeu importância em comparação com a economia de alta tecnologia, liderada pelas *Big Techs*. O colonialismo digital passou a se estruturar com base no *software*, no *hardware* e nas redes de conectividade de dados.

É importante ressaltar dois pontos fundamentais para o pensamento de Kwet. Primeiro, o *colonialismo digital* é profundamente integrado às ferramentas convencionais do capitalismo. Segundo, o controle das propriedades do mundo digital, incluindo a infraestrutura, o conhecimento e os recursos computacionais, é utilizado pelas corporações para manter os países mais pobres em uma situação permanente de dependência. Kwet considera que as *veias abertas* do Sul global (em referência a Eduardo Galeano) são, atualmente, *veias digitais*, que cruzam os oceanos. Trata-se de um ecossistema tecnológico, cuja propriedade e controle estão majoritariamente nas mãos de empresas sediadas nos EUA.

Embora não discorde por completo do pensamento de pesquisadores, como Couldry, Mejías e Zuboff (que se concentram principalmente na captura, no processamento, no uso e na rentabilidade dos dados), Kwet atribui um peso significativamente maior ao controle da propriedade das infraestruturas do digital do que esses autores.

Michael Kwet também alerta para o uso da dominação política e do exercício da violência com as tecnologias digitais. Em 2013, Edward Snowden já havia revelado como as *Big Techs* compartilham informações de inteligência com a NSA. Desde então, países na América Latina, na África e no Oriente Médio passaram a equipar suas forças militares e policiais com sofisticadas ferramentas de vigilância. Isso inclui centros de comando e controle de operações policiais, como o de São Paulo, Brasil; o uso de câmeras com reconhecimento facial nas ruas de Singapura; e a adoção de sistemas de gestão prisional no Marrocos. As Filipinas, cujo governo central implementou uma política de guerra às drogas de alta letalidade, tornaram-se um laboratório para ferramentas de vigilância e caça de procurados pela justiça.

Mais recentemente, durante a operação militar especial da Rússia na Ucrânia, iniciada em 2022, e na invasão israelense sobre a Faixa de Gaza, que começou em 2023, o uso de *drones* tornou-se uma das principais ferramentas de guerra. Também surgiram vários relatos (que carecem de confirmação) sobre o uso experimental de máquinas assassinas guiadas por Inteligência Artificial. Segundo matéria publicada pelo jornal O Globo (2024a), Israel teria utilizado IA para definir 37 mil alvos, com um cálculo de “permissão prévia” para a morte de civis.

No artigo *Digital Colonialism: US Empire and the New Imperialism in the Global South* (2018), Michael Kwet, ao citar o exemplo da África do Sul, defende que as multinacionais norte-americanas exercem um controle imperial sobre todos os níveis do ecossistema digital: *software*, *hardware* e conectividade de rede. Isso gera cinco formas de dominação:

1. O monopólio corporativo para a extração de renda e vigilância;
2. O controle das experiências mediadas por computador, impactando diretamente política, economia e cultura;
3. *Big Data* e a violação da privacidade;

4. A vigilância em massa praticada por agências de inteligência do Norte global;
5. A capacidade das elites dos EUA de persuadir parte da população a aceitar concepções de classe sobre o mundo digital, estabelecendo as bases para a hegemonia tecnológica.

No livro *Digital Degrowth: Technology in the Age of Survival* (2024), Michael Kwet mostra como as infraestruturas digitais contribuem significativamente para as mudanças climáticas, não apenas do ponto de vista do consumo de energia elétrica, mas também dos impactos da extração de minérios necessários para a fabricação de *hardware*. Na verdade, o livro é uma crítica ao crescimento sem limites do capitalismo como um todo, que ameaça a vida no planeta Terra. O autor explica que a economia digital pode parecer desconectada do mundo físico, como se houvesse uma *economia digital* e uma *economia física*. No entanto, ambas estão totalmente interligadas. *Data centers*, celulares e computadores são os dispositivos que viabilizam o acesso ao digital. Kwet propõe um *decrescimento digital* (*digital degrowth*) como parte de um conjunto de ações para evitar o aquecimento global.

1.2.2. Colonialismo de Dados

Nick Couldry e Ulises A. Mejias têm uma perspectiva mais focada do que Kwet sobre a forma atual de colonialismo. No livro *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019), a dupla apresenta o conceito de colonialismo de dados, defendendo que o centro do problema da exploração atual reside nos novos tipos de relações humanas baseadas em dados, que possibilitam a extração de informações pessoais para a geração de lucros. Nossa vida social torna-se um recurso que pode ser extraído e utilizado pelo capital como forma de acumulação de riquezas. Tanto as populações do Norte global quanto as do Sul passaram a ser fontes de informações que sustentam o capitalismo. Independente da cultura, da religião ou da ideologia política, tudo gera dados capturáveis, que são armazenados e utilizados para a formatação de perfis. As pessoas passam a considerar a captura de suas informações como algo normal, natural. Com isso, as relações sociais se

transformam, tornando-se mecanismos de extração, caracterizando um novo tipo de colonialismo.

Para os autores, o uso do termo *colonialismo* não é uma metáfora. O *colonialismo de dados* pode ser chamado assim porque, em primeiro lugar, representa uma evolução do processo histórico originado no colonialismo tradicional. Em ambos os casos, ocorre a apropriação de recursos dos colonizados, o decorrer de uma concentração altamente desigual das relações sociais e econômicas, garantindo a continuidade da apropriação de recursos, a acentuada desigualdade na distribuição dos lucros obtidos e a propagação de uma ideologia que justifica todo o processo.

No passado, havia o discurso de que os recursos eram tomados de povos considerados inferiores e que a relação colonial os ajudaria a alcançar a civilização. Hoje, algo semelhante ocorre na lógica de mercado imposta pelas grandes corporações de tecnologia e pelas consultorias. O colonialismo histórico baseava-se na extração de matérias-primas de territórios ocupados. Já o *colonialismo de dados* tem como fonte a extração das camadas da vida humana, por meio da coleta de informações sobre a saúde das pessoas, seus hábitos, costumes, preferências, trabalho, educação, consumo, relações interpessoais e familiares, além de outras ações cotidianas. Couldry e Mejías chamam isso de "*capitalização sem limites da vida humana"*.

Os autores argumentam que não se trata apenas de atribuir um novo nome ao colonialismo, mas sim de expandir o escopo do capitalismo, que teve seu desenvolvimento a partir do colonialismo histórico. O *colonialismo de dados* atua desapropriando os seres humanos até mesmo de dimensões antes inacessíveis, como o pensamento. Este é um ponto central na análise de Couldry e Mejías. No *colonialismo de dados*, a geografia assume uma configuração distinta, não se limitando apenas aos territórios físicos. A expansão ocorre não apenas de maneira externa (física), mas também interna (social).

Os autores definem "dados" como um material produzido pela abstração do mundo em categorias, medidas e representações. São blocos fundamentais para a construção de informações e conhecimentos. O monitoramento e a vigilância constantes por meio das tecnologias digitais derrubam as fronteiras entre o que é

interno ao ser humano e sua relação com o mundo exterior. Qualquer interação das pessoas com computadores ou dispositivos digitais têm a capacidade de gerar dados. A extração de dados é indiferente às origens, pois tudo pode ser sistematicamente organizado para gerar valor ao capital. E mesmo que alguém decida não utilizar qualquer equipamento eletrônico, será praticamente impossível livrar-se dos sensores espalhados pelas cidades (nas ruas, lojas, supermercados e portarias de edifícios). Criou-se um regime de vigilância que limita a autonomia dos seres humanos.

Outro ponto importante no *colonialismo de dados* é o rastreamento das relações sociais. Nunca foi tão fácil controlar a capacidade de comunicação entre indivíduos, transformando as interações em dados e explorando-as economicamente. As interações entre as pessoas tornam-se fontes de informações valiosas para a previsão de comportamentos e a modulação de escolhas. Aplicado às relações de trabalho, como na dinâmica da vida no escritório, há uma vigilância em tempo integral sobre a mão de obra. Para aqueles que dependem de ganhos obtidos via plataformas, como aplicativos de transporte urbano, como o Uber, há não apenas a precarização do trabalho, mas também um controle total sobre cada viagem realizada por motorista.

Couldry e Mejías apontam que, para tornar aceitável a concentração de poder nas mãos de poucas companhias, seja na China ou nos Estados Unidos, são criadas *Novas Ideologias Coloniais*, que produzem narrativas para desarmar resistências aos modelos de negócios. Os autores citam a *ideologia da conectividade*, que apresenta como natural o fato de pessoas, coisas e processos estarem conectados em tempo integral pela Internet. Difunde-se a ideia de que todos precisam estar *online* o tempo todo. Há também a *ideologia da datificação*, que propaga a noção de que cada aspecto da vida deve ser transferido para sistemas digitais. Existem aplicativos que monitoram até mesmo quantos copos d'água uma pessoa bebe por dia. Além disso, há a *ideologia da personalização*, que torna a vigilância mais atraente para os consumidores, adequando os *softwares* aos gostos e às preferências individuais. Em todos os casos, trata-se de um mito, uma mentira, uma *ideologia da inevitabilidade*.

Catriona Gray, da Universidade de Bath, Reino Unido, publicou o artigo *More than Extraction: Rethinking Data's Colonial Political Economy* (2023), no qual discorda frontalmente de alguns pontos e sugere complementos às ideias de Couldry e Mejías sobre o colonialismo de dados. De início, Gray considera incorreta a analogia da conversão da *"vida cotidiana em dados"* para ser explorada como *"recursos naturais"*. Segundo ela, essa comparação desconsidera processos específicos da desapropriação de dados, que não podem ser tratados como a exploração de qualquer outro recurso. Além disso, a autora acusa o trabalho de Couldry e Mejías de carecer de historicidade em relação ao colonialismo (e sua ligação com o capitalismo) até as práticas de dados atuais. Por fim, o último ponto levantado por Gray refere-se a uma oclusão epistêmica e à violência material.

1.2.3. Da violência material no colonialismo histórico

Couldry e Mejías afirmam expressamente que o *colonialismo de dados* não é uma metáfora, mas sim uma realidade: vivemos literalmente uma nova forma de colonialismo. A visão dos autores constitui uma excelente análise do momento histórico atual. Tanto que o Laboratório de Tecnologias Livres (LabLivre), da Universidade Federal do ABC (UFABC), publicou o livro *Colonialismo de Dados: Como Opera a Trincheira Algorítmica na Guerra Neoliberal* (CASSINO; SOUZA; SILVEIRA, 2021), que busca acrescentar uma perspectiva brasileira sobre o tema.

No entanto, um dos aspectos mais problemáticos na afirmação de que o *colonialismo de dados* não é uma metáfora é sua relação com a violência material, com a violência extrema observada durante o colonialismo histórico. Mesmo que se considere que as *Big Techs* atuam como instrumentos de apoio aos setores militares e de inteligência das potências globais, não se pode comparar diretamente o impacto de sua influência com as práticas genocidas das antigas metrópoles da era colonial.

Frantz Fanon é uma das personalidades mais importantes do século XX no contexto da luta anticolonial. Homem negro, psiquiatra, filósofo e revolucionário, nascido na Martinica em 1925, serviu no exército francês contra as forças do Eixo durante a Segunda Guerra Mundial. Após a derrota do nazismo, Fanon passou a

atuar pela independência da Argélia. Infelizmente, adoeceu e morreu precocemente, aos 36 anos, em 1961, sem testemunhar a vitória da libertação argelina no ano seguinte, em 1962, quando a França perdeu o domínio sobre aquele território no norte da África, que se tornou uma nação independente.

Da obra de Fanon, destacam-se dois livros: *Pele Negra, Máscaras Brancas* (1952) e *Os Condenados da Terra* (1961), leituras obrigatórias para quem se interessa pela temática anticolonialista. Com seu estilo único de escrita, Fanon nos faz sentir o peso do racismo colonial. Ele descreve como foi discriminado pelos aliados durante a segunda guerra por ser negro, ao mesmo tempo em que a resistência francesa proclamava as palavras de ordem “Liberdade, Igualdade e Fraternidade” contra as atrocidades impostas por Adolf Hitler a judeus, ciganos, pessoas com deficiência, comunistas e outros opositores. Ao ler Fanon, aprendemos que palavras abstratas, mal aplicadas, podem mascarar o peso da exploração colonial e menosprezar o sofrimento das vítimas.

Relembrar Frantz Fanon é essencial para que, ao utilizarmos a palavra “colonialismo”, não esqueçamos do que foi o colonialismo histórico real. A violência colonial teve início com a chegada de Cristóvão Colombo às Américas, em 1492. A partir daquele ano, mais de 70 milhões de pessoas pertencentes aos povos originários do continente americano foram exterminadas. Estima-se que cerca de 20 milhões tenham sido mortos no México, 18 milhões no território que hoje corresponde aos Estados Unidos, 10 milhões na região andina e outros 4 milhões no Brasil. As técnicas de execução incluíam doenças propositalmente disseminadas, fome, castigos corporais, trabalho forçado e escravidão. No colonialismo tardio na Ásia e na África, a violência não foi menor. Um dos maiores genocidas da História, Leopoldo II, rei da Bélgica, comandou o extermínio de mais de 10 milhões de pessoas no Congo entre 1885 e 1924.

Mesmo depois que as ex-colônias começaram a se tornar independentes, a selvageria colonial continuou a ser responsável por desumanidades extremas, como na África do Sul, que se tornou um Estado soberano em 1931, mas manteve um regime de segregação racial, o *Apartheid*, até 1994. A separação entre brancos (descendentes dos colonos europeus) e não-brancos (os povos africanos) era imposta de forma violenta, com respaldo legal. Em 1991, a população sul-africana

era de aproximadamente 38,9 milhões de pessoas, sendo 75% negros e apenas 14% brancos. A minoria étnica europeia, porém, controlava quase toda a riqueza do país e praticamente todo o poder político.

É justo usar a palavra “colonialismo” para descrever, no mundo digital, as novas formas de extração e exploração? Comparar essas “novas formas de colonialismo” com o colonialismo histórico, marcado pela violência extrema e por uma quantidade incomparável de mortes, sangue e sofrimento, é apropriado? Qualquer comparação deve ser feita com cuidado, para evitar esvaziar ou banalizar o verdadeiro significado do colonialismo real.

1.3. Ainda o mau e velho capitalismo

Como vimos, o uso de terminologias como “novo tipo de feudalismo” ou “novo tipo de colonialismo” gera desconfortos e imprecisões. Seria mais adequado trabalhar dentro do conceito de capitalismo para descrever sua fase atual, nesta terceira década do século XXI. Tivemos o capitalismo comercial (mercantilismo), o capitalismo industrial, o capitalismo financeiro e, agora, um capitalismo marcado pela influência e pelo protagonismo das tecnologias digitais. Mas qual seria o melhor conceito para descrevê-lo?

Couldry e Mejías buscaram responder a essa questão ao defender sua posição sobre o *colonialismo de dados*. Segundo eles, ao se referirem ao capitalismo, consideram o sistema de forma geral, e não como *capitalismo digital*, *capitalismo informacional*, *capitalismo de plataforma* ou *capitalismo de vigilância*, nem outros termos concorrentes. Os autores afirmam não estar convencidos de que o capitalismo atual seja diferente do que sempre foi: uma organização sistemática da vida para maximizar valor, resultando na concentração de poder e riqueza. Nesse sentido, aproximam-se da visão de Morozov, que argumenta que o que ocorre hoje é uma transformação dentro do próprio capitalismo.

1.3.1. Capitalismo Digital

Daniel Schiller, no livro *Digital Capitalism* (1999), foi um dos primeiros a correlacionar a Internet com o neoliberalismo. No final dos anos 1990, assistíamos ao processo de privatização das empresas de telecomunicações em diversos países, um passo necessário para a criação de novos modelos de negócio sob a lógica do neoliberalismo, que exigia mercados com menos regulamentação. A conectividade tornou-se um elemento central do mais novo segmento do capitalismo: o digital.

Havia a ideia de que a Internet era independente das infraestruturas que a mantinham funcionando e, portanto, os estados nacionais não deveriam legislar sobre a Rede, garantindo-lhe o máximo de liberdade (SILVEIRA, 2021).

Esse cenário possibilitou o florescimento de uma ampla gama de produtos e serviços *online*, começando por portais de conteúdo e lojas de comércio eletrônico, que foram a origem dos negócios baseados na Internet que vemos hoje. A rede mundial de computadores surgiu a partir de um empreendimento que uniu agências governamentais, o setor militar e instituições de ensino, tendo sido criada como parte do esforço para se precaver de uma eventual guerra contra a União das Repúblicas Socialistas Soviéticas (URSS), durante a Guerra Fria, na década de 1960. No entanto, na virada do milênio, a Rede passou a servir principalmente às corporações e à lógica expansionista de mercado.

Os governos, sobretudo nos Estados Unidos, passaram a estimular essas corporações transnacionais, ao mesmo tempo em que o ciberespaço foi percebido como um instrumento privilegiado para cultivar e aprofundar o consumismo em escala internacional, especialmente entre grupos economicamente privilegiados. Schiller (1999) escreveu, naquela época, que, ao contrário das visões utópicas e extremamente entusiasmadas sobre as potencialidades benéficas da Internet, o que ocorria era a generalização social e cultural da economia capitalista em escala global como nunca antes, tudo por meio das redes digitais. Esse fenômeno o levou a utilizar o termo *capitalismo digital*.

1.3.2. Capitalismo Cognitivo

Algo interessante a se pensar é como a Internet, criada como projeto militar, não se transformou apenas em uma arma de guerra, mas também na base das transformações do capitalismo. Foram justamente as tecnologias eletrônicas e digitais que dificultaram ainda mais a competição geopolítica para a União Soviética, que acabou sucumbindo em 1991. No entanto, não foi a Internet que levou ao fim do bloco comunista; isso ocorreu devido a diversos fatores, como o preço internacional do petróleo, a guerra do Afeganistão, a corrida armamentista com o Ocidente, a dependência dos estados satélites, a crise econômica na URSS, entre outros.

Yann Moulier-Boutang, autor de *Le capitalisme cognitif. La nouvelle grande transformation* (2007a), sustenta que o fim do socialismo real ocorreu simultaneamente à revolução da informática e da Internet. Durante o século XX, o sistema soviético teve êxito na industrialização, possibilitando a fabricação de foguetes, locomotivas, centrais hidrelétricas e armas nucleares. No entanto, a URSS enfrentou dificuldades quando começaram a despontar setores como a informática, a eletrônica e as nanotecnologias. O desenvolvimento científico e tecnológico desses novos setores, e sua posterior incorporação ao mercado, são os fundamentos do que Boutang chama de *capitalismo cognitivo*.

Progressivamente, a economia torna-se cada vez mais virtual. Os serviços e investimentos ligados à produção do imaterial ultrapassam, em volume, os recursos destinados a equipamentos materiais. O imaterial corresponde a dados, que, por sua vez, exigem captação, tratamento e armazenamento. Para Boutang, o conhecimento e a ciência assumem a liderança no sistema capitalista. São eles que impulsionam a inovação e geram novos produtos e serviços digitais. O trabalho material não desaparece, mas deixa de ser o principal ativo estratégico. Enquanto o capitalismo industrial produzia mercadorias, o *capitalismo cognitivo* gera conhecimento e dele extrai sua lucratividade.

Outro ponto essencial na obra de Boutang é como ele recupera o conceito de externalidade, originado nas ciências econômicas, mas levemente adaptado pelo autor. Externalidades são subprodutos ou resultados de uma produção conjunta entre dois ou mais entes e ocorrem quando há interdependência. Se a interação for

benéfica, ela gerará recursos, poder de ação ou bem-estar aos envolvidos, caracterizando uma "externalidade positiva". Por outro lado, se a interação reduzir esses elementos, causando danos às partes envolvidas, será uma "externalidade negativa". As externalidades podem estar fora da cadeia de produção, como, por exemplo, os custos sociais ou o dano ambiental causado por uma determinada atividade econômica. A energia elétrica é uma externalidade essencial para praticamente todos os setores de negócio. O conhecimento, a ciência e a tecnologia (inclusive as digitais), o trabalho inteligente e o trabalho realizado fora do tempo de trabalho são externalidades fundamentais nos tempos atuais. Em entrevista, Boutang explica:

> *"No capitalismo cognitivo, o que nós definimos como as externalidades (ou efeitos externos) deixam de ser marginais e ligadas a simples fenômenos parciais de indivisibilidade de bens públicos. Se o coração do valor a extrair conduz ao trabalho inteligente, inventivo e inovador e que este último mobilize a cooperação em rede dos cérebros, a captação de externalidades positivas constitui o problema número um do valor. É o trabalho fora do tempo de trabalho, é o conhecimento implícito, a capacidade de contextualização que se trata de revelar e de tratar." (Ibid., 2007b)*

A análise de Boutang remonta à primeira década do século XXI, em 2007, quando as *Big Techs* ainda estavam desenvolvendo modelos de negócios baseados na captura massiva de dados. Google e Facebook, por exemplo, eram relativamente recentes e ainda não haviam assumido a forma que têm atualmente. Com o surgimento das grandes plataformas digitais, as empresas passaram a se apoiar nos dados capturados de seus usuários, além da própria produção de conteúdo, realizada por quem as utiliza. O autor foi bastante preciso ao visualizar, de forma antecipada, o trabalho voluntário dos usuários como uma externalidade positiva para as *Big Techs*.

1.3.3. Capitalismo de Vigilância

Pouco mais de uma década após Boutang conceber o termo *capitalismo cognitivo*, o mercado das *Big Techs* já tinha o formato que, em grande parte, vemos hoje: captura em massa de dados, tratamento e comercialização de informações processadas a partir deles. Em 2015, Shoshana Zuboff publicou o artigo *Big Other:*

Surveillance Capitalism and the Prospects of an Information Civilization, que posteriormente evoluiria para o livro *The Age of Surveillance Capitalism* (2019).

Zuboff testemunhou o surgimento do que as grandes companhias chamam de *Big Data*, um conjunto tecnológico que reúne grandes quantidades de dados em diferentes formatos e que circulam em alta velocidade. Qualquer fonte de dados pode ser aproveitada para o *Big Data*: portais *web*, redes sociais, transações *online*, sensores, dispositivos conectados à Internet, entre outros. A principal característica do *Big Data* é sua capacidade de extrair e analisar dados para diversos fins. Zuboff adverte sobre as consequências desse processo: quanto mais dados são gerados sobre os indivíduos, maior será o controle sobre as pessoas.

Para a autora, é um erro olhar o *Big Data* apenas pelo viés técnico. Não se trata de uma tecnologia inevitável que surge de um processo autônomo. Ou seja, não é verdade que se o sistema não operasse da forma como opera, simplesmente não existiria. Segundo ela, a forma de operação do *Big Data* é intencional e decorre de uma nova lógica de acumulação de capital, que ela denomina como *capitalismo de vigilância*. Ao capturar, processar e armazenar dados em massa, as empresas capitalistas passam a ter o poder de prever e modificar o comportamento humano para gerar receita e controlar mercados.

Zuboff também cria um novo termo para explicar esse mecanismo de vigilância contínua: *Big Other,* uma referência direta ao *Big Brother*, o Grande Irmão, do livro *1984*, escrito por George Orwell. Trata-se de um romance ficcional sobre uma sociedade distópica totalitária, cujo líder exerce controle absoluto sobre todos os aspectos da vida dos cidadãos e das cidadãs. O *Big Other*, criado pelo atual *Big Data*, torna o *Big Brother* de Orwell algo frágil. O *Big Other* está presente em todos os lugares da sociedade em rede e tem o potencial de capturar todas as nossas informações, processá-las e estabelecer novas formas de lucro. Gera um novo regime que aniquila a privacidade e a liberdade individual.

Mais recentemente, a fome das *Big Techs* por dados tem impulsionado o processo conhecido como *transformação digital*. A propaganda corporativa busca persuadir empresas tradicionais, que ainda não completaram sua integração total ao mundo digital, a incorporarem mais tecnologia e a se tornarem mais dependentes das fornecedoras. Em um publieditorial (CNN Brasil, 2022) intitulado *“IBM impulsiona*

os negócios para se tornarem Data Driven”, a *Big Blue* tenta convencer que empresas que trabalham seus dados são mais competitivas, têm mais segurança na tomada de decisões e conseguem inovar com mais eficiência. Por meio do *marketing*, o objetivo da IBM é aumentar suas vendas, algo inerente ao mundo dos negócios. No entanto, fica explícito que a empresa deseja ser contratada e remunerada para processar dados de terceiros. Ela lucra não apenas com as receitas advindas dos contratos, mas também com o acesso privilegiado aos dados, que servirão para alimentar suas bases e seus modelos de Inteligência Artificial.

A terminologia criada por Shoshana Zuboff não é um consenso entre os pesquisadores da área. Couldry e Mejías acreditam que, embora a vigilância seja uma parte essencial do sistema atual, ela não tem força suficiente para rebatizar o capitalismo como *capitalismo de vigilância*. A dupla argumenta que, desde o controle das pessoas escravizadas na época colonial até a gestão do trabalho dos operários na sociedade industrial, a vigilância sempre esteve presente no capitalismo.

1.3.4. Capitalismo de Plataforma

Na mesma época em que Zuboff escrevia sobre o *capitalismo de vigilância*, o pesquisador Nick Srnicek também analisava esses fenômenos, mas com um enfoque diferente: a precarização do trabalho por meio da plataformização da sociedade. Quando lançou seu livro *Platform Capitalism* (2017), já estavam na moda os termos utilizados pelas consultorias de mercado, como *gig economy* (algo como *economia do bico*) ou *Quarta Revolução Industrial*. O *marketing* corporativo tentava (e continua tentando) vender esses movimentos como fontes de empreendedorismo e flexibilidade. Na prática, representam uma mudança na relação entre trabalhadores e capital: enquanto os primeiros veem seus direitos desaparecerem, as empresas encontram novas formas de lucrar.

Assim como os outros autores já citados, Srnicek vê a economia digital tornar-se mais relevante neste século XXI do que as indústrias tradicionais. O declínio da lucratividade da produção fabril tem levado o capitalismo a focar nos dados como a única forma de sustentar o crescimento econômico. A economia baseada em dados transformou-se no ponto central das relações entre trabalhadores, clientes e

capitalistas. Os trabalhadores tornam-se altamente vulneráveis a condições de trabalho com elevado grau de exploração e, em muitos casos, esses novos negócios representam sua única possibilidade de obter alguma renda.

As plataformas, abastecidas por bases de dados valiosas que apenas elas possuem, passam a oferecer serviços digitais como intermediárias de segmentos de mercado, entregando interfaces fáceis e rápidas por meio dos dispositivos que todos têm em mãos, principalmente os *smartphones*.

Um dos modelos de plataformas mais conhecidos, frequentemente usado como sinônimo da plataformização, é o Uber (uberização), que conecta motoristas particulares a passageiros por meio de um aplicativo. A Uber atua como intermediária: não possui frota de veículos nem motoristas contratados. O que ela faz é aproveitar a infraestrutura existente nos centros urbanos (carros, ruas, avenidas) e a necessidade dos clientes e a carência financeira dos donos de automóveis. Desses motoristas, a empresa cobra um percentual sobre as tarifas, que varia entre 20% e 30% do valor das corridas.

Cada corrida gera novos dados para o aplicativo. Com isso, a Uber pode aprimorar continuamente seus algoritmos para otimizar rotas, reduzir tempos de espera e ajustar preços de acordo com a demanda do momento (preços dinâmicos). Como a empresa opera em escala global, também se beneficia da escalabilidade e da diversificação dos mercados nos quais atua.

Os motoristas são submetidos a um sistema de avaliação, pelo qual recebem notas dos passageiros após cada viagem. Aqueles que forem mal avaliados por uma quantidade preestabelecida de clientes poderão ser excluídos da plataforma, na maioria das vezes sem direito de defesa. Se essa era sua única forma de obter dinheiro, simplesmente deixa de existir, e sem qualquer direito trabalhista a receber. O projeto declarado da empresa, no entanto, é eliminar definitivamente a necessidade de motoristas. A Uber investe pesadamente para, no futuro, operar com carros autônomos, eliminando o fator humano da prestação de serviços.

A Uber vem realizando testes com carros autônomos. Segundo Faustino (2023), a empresa já opera com veículos sem condutores humanos nos Estados Unidos. Na região de Phoenix, já é possível realizar viagens com os "carros-robô", graças a uma parceria entre a Uber e a Waymo, empresa de veículos autônomos da

Alphabet (controladora do Google). De acordo com o site *oficial* da Waymo, no final de 2024, já ocorriam mais de 100 mil viagens por semana em São Francisco, Phoenix e Los Angeles. Para 2025, os planos incluem a expansão do serviço para Austin e Atlanta (WAYMO, 2024).

Além do transporte urbano, há plataformas desenvolvidas para diversos setores empresariais, como publicidade, computação em nuvem, automação industrial, comércio eletrônico e produtos sob demanda. O Airbnb é uma plataforma de hospedagem que conecta proprietários de imóveis a hóspedes. A Amazon tornou-se um poderoso *marketplace* que conecta vendedores e compradores. O iFood é uma plataforma de entrega de alimentos a domicílio. O Google é uma plataforma de busca que lucra ao conectar anunciantes e usuários.

1.3.5. Dataficação, dataísmo e vigilância de dados

Sérgio Amadeu da Silveira (2021) propõe uma atualização do conceito de *capitalismo digital*, analisando as mutações da economia informacional para a economia digital baseada em dados, além de ressaltar a influência do neoliberalismo nesse processo de digitalização da economia e da sociedade. O *capitalismo digital*, conforme proposto por Schiller, transforma-se em um *capitalismo digital-dataficado* (*dataficação*), impulsionado pela emergência das plataformas e pelo tratamento massivo de dados.

Recuperando os escritos da pesquisadora José Van Dijck (2014), Silveira explica como estamos caminhando para uma sociedade que deposita total confiança nos dados. De maneira quase generalizada, a sociedade global passa a acreditar que a quantificação dos dados é objetiva e, portanto, supostamente “sem falhas”. Além disso, assume-se que todo comportamento humano é rastreável e passível de digitalização. Van Dijck denomina essa crença *ideologia do dataísmo*.

O problema surge quando agentes institucionais, como juízes de direito, forças policiais e militares, políticos, empresários e tomadores de decisão, aderem ao *dataísmo* e passam a confiar quase integralmente nos dados coletados e interpretados a partir da Internet, das mídias sociais e das tecnologias digitais. Há uma grande possibilidade de que vieses discriminatórios nos algoritmos prejudiquem

grupos minoritários como consequência de decisões equivocadas induzidas pelos sistemas digitais.

Van Dijck propõe um novo conceito para se referir a essa vigilância constante por meio do uso de (meta)dados: o *dataveillance*. Essa vigilância de dados remete às proposições de Shoshana Zuboff e ao seu conceito de *capitalismo de vigilância*. O *dataveillance* consiste na prática de monitoramento e coleta de dados *online*, incluindo metadados, permitindo, assim, a vigilância contínua das comunicações dos usuários e de suas interações em diversas plataformas, como cartões de crédito, sistemas GPS, e-mails e redes sociais.

Uma das diferenças entre Van Dijck e Zuboff é o peso atribuído à importância dos metadados pela primeira nesse sistema de vigilância. Metadados são dados sobre outros dados. Por exemplo, em uma fotografia digital, o conteúdo específico (a foto em si) é o que interessa ao usuário. No entanto, junto com o mapa de *pixels* que dá forma à imagem, podem estar embutidas informações como a data em que foi tirada, o tipo de câmera utilizada e a resolução da figura. Essas informações, que compõem esse “cabeçalho”, são os metadados.

Os metadados são essenciais para uma categorização eficiente de aplicações, como as de Inteligência Artificial. Em 13 de maio de 2024, a empresa OpenAI anunciou o lançamento da ferramenta de IA chamada ChatGPT-4o, um modelo de linguagem projetado para compreender e gerar texto de forma altamente semelhante à comunicação humana. O sistema pode responder perguntas, criar conteúdos, auxiliar em traduções, entre outras funções (OpenAI, 2024). O sucesso do produto gerou um frenesi midiático, tornando o uso da IA possivelmente o tema daquele ano na área de tecnologia, dominando a pauta de jornais, revistas, telejornais, portais *web* e influenciadores digitais especializados.

Do ponto de vista do debate sobre *soberania digital*, a Inteligência Artificial representa mais um desafio. Além de compartilhar com os *softwares* tradicionais as mesmas barreiras de entrada impostas pelas grandes corporações, a IA também é capaz de criar e editar seus próprios códigos, o que, em muitos casos, dificulta até mesmo para os desenvolvedores humanos a compreensão exata do que está sendo processado.

CAPÍTULO 2
DA SOBERANIA

Soberania é um tema fundamental na Ciência Política clássica. Maquiavel, em *O Príncipe* (1532), dedica-se a descrever o Estado de sua época, as formas de governo e os procedimentos úteis para a gestão do poder. Embora Maquiavel não tenha formulado uma teoria específica sobre a soberania, sua obra é centrada no soberano: como fazer com que seu poder seja aceito e reconhecido, como administrar alianças e como evitar rebeliões.

O conceito de soberania foi tratado por Jean Bodin no final do século XVI, com a publicação de Os *Seis Livros da República* (1576). Bodin propõe-se a investigar as ações humanas e suas vontades, tais como o desejo por sobrevivência, a organização da vida social, o desenvolvimento civilizatório e a satisfação dos sentidos do espírito. Tais necessidades só poderiam ser supridas pelo estabelecimento de uma comunidade política e, consequentemente, torna-se determinante o estabelecimento de regras, seja no âmbito moral, familiar ou civil. Para que se possa governar a comunidade política, é preciso garantir instrumentos ao soberano, como promulgar e revogar leis, declarar guerra, atribuir penas e recompensas. Surgem, então, os *"direitos de soberania"*, o comando supremo (*summum imperium*).

O tema da soberania também é tratado pelos contratualistas Thomas Hobbes, John Locke e Jean-Jacques Rousseau, que defendem a ideia de um contrato social para estabelecer o Estado. No entanto, há diferenças fundamentais entre eles, que mostram como a palavra soberania é um termo que evolui com a história. Como explica Fernandes (2020), Hobbes, ao buscar justificar o poder absoluto dos reis, vê a soberania como ilimitada, despótica, definitiva, irrevogável e indivisível. Locke, avançando para o pensamento liberal e retomando as ideias de Montesquieu, propõe a soberania como divisível entre poderes. A soberania deve ser restrita e pode ser revogada. O poder deve ser separado em Executivo, Legislativo e Judiciário. Rousseau vê a soberania como pertencente ao povo, enquanto corpo moral coletivo, e acredita que deve ser governada de maneira democrática, pela expressão da *vontade geral*.

Durante o século XX, mais precisamente nas décadas de 1930 e 1940, período de ascensão do nazismo alemão, Carl Schmitt retoma o pensamento de Bodin e Hobbes ao propor uma concepção política decisionista totalitária (MACEDO JÚNIOR, 1997). Schmitt critica a democracia liberal e argumenta a favor da ditadura como forma de superação da indecisão política, aproximando-o do pensamento de Adolf Hitler.

Com o final da Segunda Guerra Mundial, a democracia liberal passa a ser impulsionada pela liderança dos Estados Unidos e do mundo ocidental como um valor fundamental. A *Declaração Universal dos Direitos Humanos* (1948) afirmará a vontade popular como base da autoridade governamental e a necessidade da realização de sufrágio universal periodicamente. A promoção da democracia passa a ser um argumento para o combate ao comunismo no mundo, dando aos EUA pretextos para intervenções diretas ou indiretas na política interna de outros países.

No pós-Segunda Guerra, os Estados Unidos mantiveram ou estabeleceram bases militares onde havia interesse geopolítico, principalmente devido à Guerra Fria e à disputa com a União Soviética. Um dos locais para onde foram enviados pessoal e equipamentos bélicos foi a Líbia, que proclamou sua independência do Reino Unido em 24 de dezembro de 1951. Segundo Heefner (2015), em outubro daquele mesmo ano, um telegrama enviado por um comandante militar dos EUA em Trípoli para o Departamento de Estado norte-americano, comentando sobre a presença militar na base aérea Wheelus Field, em território líbio, usou a expressão: *“a slice of their sovereignty”* (*uma fatia da soberania deles*, tradução livre).

Mesmo após o colapso do bloco comunista, no início dos anos 1990, os Estados Unidos continuaram a “promover a democracia” em outras partes do mundo. As bases da doutrina de política externa que justificam a exportação de democracia pelo uso da força (e sua alegada relação com a segurança nacional norte-americana) foram se adaptando ao longo do tempo. Em muitos momentos, nos discursos oficiais, as palavras “democracia” e “segurança” tornam-se intercambiáveis, sendo utilizadas quase como sinônimos.

2.1. A Guerra dos Trinta Anos e a Soberania Estatal como a conhecemos

A transição do feudalismo histórico para o capitalismo mercantilista não foi marcada somente por mudanças de caráter econômico, mas também por transformações políticas e religiosas. A Guerra dos Trinta Anos, entre 1618 e 1648, foi um conflito devastou o velho continente, abrangendo os principais territórios de suas regiões central e ocidental (PORTUGAL, 2025). Como beligerantes, tivemos o Sacro Império Romano-Germânico, os Estados Imperiais, a França, o Império Espanhol, a Suécia, as Províncias Unidas dos Países Baixos, a Confederação Helvética, a República de Veneza e o Papado. Enfim, praticamente todos os territórios europeus relevantes.

A razão do conflito foi o crescente poder dos protestantes em detrimento da tradição da Igreja Católica, que exerceu forte influência sobre a nobreza europeia por séculos, durante todo o período medieval, limitando o poder dos reis. Com as monarquias nacionais em processo de fortalecimento, a Reforma Protestante foi uma solução para aqueles que desejavam minar o poder do alto clero, subordinado ao Papa, em Roma. O epicentro da Guerra dos Trinta Anos foram as terras onde hoje está a Alemanha. O conflito começou entre o rei católico do Sacro Império Romano-Germânico e os Estados Imperiais protestantes, mas envolveu Portugal, Espanha, França, Hungria, Transilvânia, Dinamarca e Inglaterra, apenas para citar alguns dos povos em batalha nessa guerra destrutiva, cujas estimativas apontam para cerca de 8 milhões de mortos, possivelmente algo em torno de 10% a 15% da população europeia viva na época.

Para pôr fim à Guerra dos Trinta Anos, firmou-se uma série de tratados que vieram a ser conhecidos como “Paz de Vestfália”, em 1648. No campo das Relações Internacionais, a Paz de Vestfália é vista como o embrião da noção de equilíbrio de poder entre estados, do estabelecimento do “Estado-nação” e apresenta os princípios de soberania estatal nos moldes como os conhecemos hoje (CERVO, 2007, p. 63). Costuma ser vista como um marco inicial do Direito Internacional clássico.

Nos séculos que se seguiram, nos vários confrontos que ocorreram em solo europeu ou entre nações europeias, em especial após as Guerras Napoleônicas (1803-1815) e a Primeira Guerra Mundial (1914-1918), manteve-se a prática de usar tratados entre nações como forma de definir as regras entre vencedores e derrotados. Com a Segunda Guerra Mundial não foi diferente e, rendidas a Alemanha nazista e as potências do Eixo, ocorreram conferências, como Yalta e Potsdam, em 1945, que impuseram os termos dos vitoriosos aos derrotados. Nesse contexto, nasceu a Organização das Nações Unidas (ONU).

Os vencedores do conflito organizaram o sistema ONU como forma de consolidar uma nova ordem, com a qual os demais países deveriam se comprometer. O objetivo declarado pelas novas lideranças globais para a criação das Nações Unidas era evitar que os horrores da guerra se repetissem. Criaram-se compromissos internacionais para que obrigações decorrentes de tratados e de outras fontes do direito internacional fossem respeitadas, refundando uma governança global, supostamente focada na resolução de conflitos pela diplomacia e não no confronto bélico. Em seu documento fundacional, a *Carta das Nações Unidas* (1945) trata explicitamente de soberania apenas uma vez, usando a palavra “soberana” como oposição à “tutela” de um país sobre outro.

> *“ARTIGO 78 - O sistema de tutela não será aplicado a territórios que se tenham tornado Membros das Nações Unidas, cujas relações mútuas deverão basear-se no respeito ao princípio da igualdade soberana”*. (ONU, 1945).

O Sistema Internacional de Tutela foi criado inicialmente para gerir territórios afetados pelo decorrer da 2ª Guerra, sobre os quais havia dúvidas acerca de eventuais separações das nações que antes os controlavam. Porém, o mecanismo foi mantido disponível para eventual uso futuro, caso fosse necessário, desde que contasse com o apoio do Conselho de Segurança da ONU. A tutela poderia ser aplicada para favorecer a paz e a segurança internacionais ou estimular o respeito aos direitos humanos e às liberdades fundamentais para todos. Atualmente, são tutelados 11 territórios, como Samoa Ocidental, Ruanda-Urundi, partes de Camarões e Togo, Nova Guiné e Nauru, entre outros (ONU, 2025).

Atualmente, o mundo vive um período de enfraquecimento do sistema ONU e do multilateralismo, marcado pela Operação Militar Especial da Rússia na Ucrânia (2022) e pelo conflito Israel-Gaza (2023). Nesses casos, o Conselho de Segurança da ONU foi ignorado ou relegado a segundo plano, enfraquecendo a instituição.

A República Federativa do Brasil, país-membro das Nações Unidas, menciona a palavra “soberania” com destaque no Artigo 1º da Constituição de 1988:

> *Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:*
>
> *I - a soberania;*
> *II - a cidadania;*
> *III - a dignidade da pessoa humana;*
> *IV - os valores sociais do trabalho e da livre iniciativa;*
> *V - o pluralismo político.*
>
> (BRASIL, 1988)

Na abertura da 79ª Assembleia Geral da ONU, em 2024, o Presidente do Brasil, Luiz Inácio Lula da Silva, declarou que, dentre os elementos essenciais da soberania, estão incluídos *“o direito de legislar, julgar disputas e fazer cumprir as regras dentro de seu território, incluindo o ambiente digital”*. Focando-se no tema da Inteligência Artificial, o presidente brasileiro destacou a consolidação das assimetrias que levam ao oligopólio do saber e pediu uma IA que fortaleça a diversidade cultural, que *“também tenha a cara do Sul Global”* (LULA DA SILVA, 2024).

O discurso do Presidente Lula foi influenciado por um episódio que precedeu sua ida à ONU: os embates entre a rede social X (ex-Twitter) e o poder judiciário brasileiro. A empresa, propriedade do bilionário Elon Musk, insurgiu-se contra as decisões do Supremo Tribunal Federal (STF), a mais alta instância do judiciário, e acabou sendo bloqueada no país por cerca de 40 dias, no final de agosto de 2024. A X, por fim, dobrou-se às determinações do STF, mas houve momentos de tensão social e política (FALCÃO; BUSTAMANTE, 2024). Um dos resultados do embate foi que, além do banimento temporário da rede social X, o governo brasileiro, na época, passou a manifestar a intenção de diminuir sua dependência tecnológica.

Alguns dos maiores intelectuais do planeta e pesquisadores da sociedade da informação divulgaram a *CARTA PÚBLICA CONTRA O ATAQUE DAS BIG TECHS À SOBERANIA DIGITAL*[1], em 14 de setembro de 2024. São signatários nomes como Cédric Durand, Evgeny Morozov, Francesca Bria, Jose van Dijck, Mariana Mazzucato, Nick Couldry, Nick Srnicek, Paola Ricaurte Quijano, Sérgio Amadeu da Silveira, Shoshana Zuboff, Thomas Piketty, Ulises Mejias e Yanis Varoufakis.

A carta pública trouxe luz ao tema, frequentemente negligenciado por parte das autoridades da República. A carta pública expressa a preocupação dos que a elaboraram com os ataques das *Big Techs* e de seus aliados contra a *soberania digital* do Brasil, afirmando que a disputa do judiciário brasileiro contra a empresa X é apenas mais um dos esforços das megacorporações para restringir a capacidade das nações soberanas de definirem uma agenda de desenvolvimento digital livre.

A carta também afirma que é preciso um *"espaço digital suficiente para que os estados possam direcionar as tecnologias colocando as pessoas e o planeta à frente dos lucros privados ou do controle unilateral do Estado"* e destaca a necessidade de se desenvolver princípios básicos de regulamentação na ONU.

Um fato assustador que chamou a atenção em meio às repercussões pós-bloqueio da rede social X foi a divulgação, pelo portal Poder360 (2024a), do OFÍCIO nº 16-A4.7/A4/GabCmtEx1, do Comando do Exército brasileiro, datado de 6 de junho de 2024 (BRASIL, 2024a). É importante ressaltar que o bloqueio da X ocorreu em agosto, logo, o documento foi produzido com mais de um mês de antecedência à decisão judicial. No ofício, afirma-se que o cancelamento do contrato com a Starlink (empresa também de propriedade de Musk) geraria prejuízo para o emprego de tropas especializadas, pois a empresa proporciona *"redundância operacional, elevada confiabilidade, rapidez de instalação, altas taxas de banda, cobrindo grandes distâncias com praticamente nenhuma interferência do terreno ou das condições atmosféricas [...]."* Em outro trecho, o documento diz que a Starlink possibilita *"a devida prontidão estratégica."* Ou seja, o Exército brasileiro depende de uma empresa norte-americana de satélites de baixa órbita para proteger a soberania da Amazônia brasileira.

1 FONTE: Carta pública contra o ataque das *Big Techs* à *soberania digital*, 14 de setembro de 2024: https://capitaldigital.com.br/wp-content/uploads/2024/09/Brazil-Letter-fv_240914_PT.pdf

Na verdade, quem ameaça a soberania brasileira é a Starlink. Não há possibilidade de verificação e controle pelas autoridades nacionais sobre o que os equipamentos em órbita podem, de fato, fazer. Cada satélite da Starlink pode carregar até duas câmeras, que, supostamente, servem para observar estrelas, corpos celestes ou condições atmosféricas. No entanto, essas câmeras poderiam ser redirecionadas para a Terra, capturando imagens de resolução média (PPLWARE, 2024). A Figura 2 mostra uma postagem da Starlink na rede social X com uma foto tirada por um de seus satélites.

Figura 2 – Vista de um eclipse solar de um satélite Starlink em órbita

Fonte: @Starlink em X.com

De acordo com Vaidhyanathan (2023), uma demonstração de poder da Starlink foi a decisão de Elon Musk de não estender a conectividade de seus satélites sobre as áreas ucranianas que estavam sob controle do exército russo, como o Donbass. Nesses territórios, a Internet foi cortada. Musk afirmava não querer

uma escalada no conflito. Porém, com que direito um empresário sul-africano pode decidir sobre questões civis e militares do conflito no Leste Europeu?

Em março de 2025, o Presidente Lula usou a expressão *“colonialismo digital”* para pedir a criação de um *"arcabouço jurídico sólido"* para proteger a população da *"concentração sem precedentes das oligarquias digitais”* e do poder das *Big Techs*. O contexto da declaração ocorreu na posse do Presidente da Ordem dos Advogados do Brasil (OAB), quando Lula comentava a tentativa de golpe de Estado em 8 de janeiro de 2023 por militantes de extrema direita e afirmava que era necessária uma regulamentação das redes sociais (COUTINHO, 2025).

A cooperação internacional que possibilita a Governança da Internet também está ameaçada pelo poder crescente das *Big Techs*. Ainda que não seja um instrumento de multilateralismo clássico, mais associado aos estados nacionais e às organizações internacionais, a Governança da Internet é um exemplo de como pode funcionar a colaboração entre governos, poderes locais, empresas, comunidade científica-tecnológica e entidades da sociedade civil organizada.

Como explica Marília Maciel (2021, p. 6-17), o termo *“governança”* não tem a mesma compreensão em todos os países, sendo que alguns associam a palavra à autoridade ou ao governo. Mesmo assim, outras nações a associam à legitimidade dos participantes, àqueles que têm algo a contribuir com as discussões, que têm prática, experiência e recursos a serem aportados. Um modelo multissetorial de governança busca a harmonia da participação dos atores. Porém, Maciel alerta que a disputa tecnológica entre EUA e China tem levado ao que se chama *“forum shifting”*, que é quando um grupo move sua agenda de uma organização para outra, com o objetivo de discutir um determinado tema ou encaminhar deliberações onde lhe sejam mais favoráveis. Esvazia-se ou mesmo abandona-se o fórum de debate e decisão cujo resultado desejado terá mais dificuldade de ser aceito.

2.2. Dinâmica geopolítica global em 2025

Antes de prosseguir, faz-se necessária uma pequena contextualização sobre o que está acontecendo no planeta no momento em que esta tese é escrita. Isso porque vivemos em um período da humanidade em que as tensões e disputas entre

países são crescentes. A necessidade de espionagem é tão grande quanto ou maior do que a que vimos no período da Guerra Fria, com o agravante de que as tecnologias de espionagem nunca foram tão poderosas.

O mundo em 2025 é um lugar onde o sistema de regras internacionais que vigorou desde o final da Segunda Guerra Mundial está fortemente ameaçado (COLLETTA, 2024). De um lado, há a ascensão chinesa como potência econômica e militar. De outro, os Estados Unidos modificam suas políticas externa e comercial para tentar reagir ao crescimento chinês.

Em 2022, a Federação Russa invadiu a Ucrânia e ocupou vários territórios daquele país. Desde 2023, Israel realiza uma guerra de aniquilação contra a Faixa de Gaza, na Palestina. Israel também atacou o Hezbollah no Líbano, lançou ataques aéreos contra o Irã e teve participação na derrubada de Bashar al-Assad do governo da Síria. Israel e os EUA também combatem os rebeldes houthis no Iêmen (GARDNER, 2025).

O presidente dos EUA, Donald Trump, fala abertamente nas mídias sobre seu interesse em anexar territórios, como a dominação da Groenlândia (região autônoma da Dinamarca) ou a retomada pelos EUA do Canal do Panamá. Entre bravatas e ameaças, Trump sugeriu a anexação do Canadá aos Estados Unidos e prometeu atacar o México militarmente para conter o crime organizado (BISCHOFF, 2025).

Tendo Canadá, México e China como alvos iniciais, Donald Trump anunciou em 2 de abril de 2025 um “tarifaço” contra 180 países, aumentando as tarifas de importação dos Estados Unidos, o que fez as bolsas de valores despencarem em todo o mundo (G1, 2025).

A tensão no Mar do Sul da China também é elevada, com o temor cada vez maior de uma invasão da República Popular à ilha de Taiwan, considerada por Pequim uma “província rebelde” (BLOOMBERG, 2025). A China também lançou um enorme projeto de infraestrutura para ligar a Ásia, o leste da África e o leste da Europa, tanto por terra quanto por mar, chamado de Cinturão Econômico da Rota da Seda – ou nova Rota da Seda (WONG, 2023). Ao mesmo tempo, os EUA, a União Europeia, a Índia e a Arábia Saudita trabalham em um corredor econômico alternativo (SIC NOTÍCIAS, 2023).

Assistimos ao uso intensivo e progressivo da Inteligência Artificial em quase todas as áreas, inclusive como arma de guerra (AFP, 2023). A Europa planeja ampliar significativamente o seu orçamento militar e se rearmar fortemente contra uma possível agressão russa, em um momento em que os EUA se afastam da OTAN (LENDON, 2025). Trump é politicamente próximo de Putin, assim como de líderes globais de uma extrema direita em crescimento pelo mundo. Entre os expoentes desse movimento estão a Hungria de Viktor Orbán, a Itália de Giorgia Meloni (PADINGER, 2022) e a Argentina de Javier Milei. Essa extrema direita se vale das *Big Techs*, em especial das redes sociais, para promover a desinformação e mobilizar apoios.

As mudanças globais têm feito com que o multilateralismo e a resolução de conflitos pela via diplomática estejam em um momento de declínio. A opção pela força, inclusive à margem do sistema ONU, parece ter se tornado uma opção cada vez mais viável e presente. Em um mundo assim, a confiança em contratos comerciais entre empresas baseadas em países diferentes precisa ser relativizada. Se as nações estão dispostas à guerra, ao bombardeio, e à morte, o que é para elas romper algumas linhas de compromissos jurídico-burocráticos?

2.3. *Soberania digital* e *soberania de dados*

Entendemos o que é a soberania histórica, que é a qualidade ou estado do que é soberano. Refere-se à autoridade de um líder sobre um território e seu povo, ou sobre um conjunto de poderes de um Estado organizado politicamente que tenha autoridade plena no plano interno. Para que tenha status de nação, no arranjo geopolítico mundial atual, o Estado precisa ser reconhecido por outras nações, em especial pelos membros da Organização das Nações Unidas. Porém, quando falamos de *soberania digital*, o que isso significa exatamente?

O termo *soberania tecnológica* surgiu em 1967, utilizado pelo Conselho de Ciência do Canadá como ação indispensável para aumentar e controlar a capacidade de criar tecnologias como elemento da soberania nacional (GLOBERMAN, 1978, p. 43) e tem se desdobrado em novas interpretações desde então. Como escrevem SCHIAVI e SILVEIRA:

> *“As transformações sociotécnicas e econômicas advindas da emergência das tecnologias de informação e comunicação (TICs), o avanço das máquinas cibernéticas, a expansão da Internet, serão a base do surgimento de novas abordagens da soberania e do uso da expressão soberania digital”*. (SCHIAVI; SILVEIRA, 2022, p. 6)

O conceito de *soberania digital* está em disputa e se confunde, dependendo de quem o utiliza e como o utiliza. Couture e Toupin (2018), a partir de uma extensa pesquisa bibliográfica, dividiram em cinco categorias os usos mais comuns do termo *soberania digital* (ou alguma de suas variantes[2]). São elas: 1. soberania tecnológica de Estado e nacional; 2. soberania tecnológica e movimentos sociais; 3. soberania tecnológica indígena; 4. soberania tecnológica pessoal; e 5. tecnologia como um meio para a soberania. Em síntese, a visão de soberania estatal é apenas uma das possibilidades quando se trata de *soberania digital*. Também se percebe que o poder econômico e os ativistas sociais têm visões muito diferentes sobre o que significa o conceito.

Como exemplo dos vários tipos de visão, um artigo no site do Fórum Econômico Mundial considera que *“soberania digital, soberania cibernética, soberania tecnológica e soberania de dados referem-se à capacidade de ter controle sobre seu próprio destino digital – os dados, hardware e software nos quais você confia e cria”* (FLEMING, 2025).

O setor privado prefere usar a expressão *soberania de dados* a *soberania digital*. As empresas abordam o assunto geralmente quando se discutem diferenças regulatórias entre diferentes países ou quando querem vender produtos e serviços que supostamente reduzem os riscos de soberania no meio digital. A falta de padronização legislativa é um problema para as corporações, pois torna mais desafiadora a tarefa de manter e aprimorar suas soluções, adequando-as aos regramentos locais.

Corporações como a IBM vão definir *soberania de dados* como *“dados armazenados e processados no país onde foram gerados”*. Segundo o portal *web* da empresa, *soberania de dados* consiste em:

---

2 NOTA DO AUTOR: Couture e Toupin (2018) listam algumas variantes do conceito “*soberania digital*”, que aparecem em vários autores: *Technological sovereignty; Digital sovereignty; Network sovereignty; Data sovereignty; Spectrum sovereignty; Internet sovereignty; Cyber sovereignty; Computer sovereignty; Network sovereignty; Information sovereignty.*

> *“[…] parte central das estratégias legais, de privacidade, segurança e governança para empresas que lidam com o armazenamento, processamento e transferência de dados. Ter uma abordagem robusta para a gestão de dados e fluxos internacionais de dados — um componente-chave da soberania de dados — ajuda as organizações a proteger suas informações mais sensíveis de ataques cibernéticos e outras ameaças”*.
> (FLINDERS; SMALLEY. [IBM], 2024)

Segundo Goovaerts (2024), executivos do Google reconhecem o crescimento da tendência de adoção de redes soberanas. Admitem que as regulamentações por *soberania digital*, ou movimentos para que se adotem regulamentações, não se restringem mais à União Europeia, onde tudo começou, mas também na Índia, Japão e Austrália, além de iniciativas no Oriente Médio e na África.

Para Archana Ramamoorthy, uma das executivas do Google entrevistadas por Goovaerts, a importância da *soberania digital* no mundo tende a aumentar. No entanto, os governos deverão equilibrar o que querem manter como dados privados e quais dados podem ser utilizados para *“avançar com suas economias”*. Para ela, trata-se de uma *“questão cultural”*, e que o conceito de soberania pode mudar, tornando mais fácil a evolução do cenário regulatório. Ou seja, podemos interpretar as palavras de Ramamoorthy da seguinte forma: se estiver difícil de cumprir com as obrigações pelo que se entende como soberania, mudemos o conceito.

Galij, Pawlak e Grzyb (2024, p. 4) fizeram uma ampla pesquisa na literatura acadêmica e identificaram que há três visões principais sobre *soberania de dados*: 1. aspectos legais, particularmente regulamentações internacionais; 2. estratégias para gerenciamento de dados de governo e do poder público; e 3. soluções técnicas, variando de ferramentas experimentais até produtos prontos para comercialização. Boa parte dos debates se relaciona a formas de padronização internacional.

Simona Levi, em *Digitalización Democrática: soberania digital para las Personas* (2024), propõe um olhar diferente para a soberania no mundo digital, alertando que o problema nos dias atuais é se a digitalização está sendo democrática ou não, e se está sendo benéfica para a maioria da população global. Ela levanta a ideia de *soberania digital das pessoas*, não apenas de uma *soberania digital* atrelada aos Estados nacionais, em sentido geopolítico. Trabalha a *soberania digital* como o direito à privacidade individual, como soberania dos dados das pessoas e de grupos, bem como sua proteção legal efetiva, livres de vigilância em

massa e de rastreamento, exercendo o direito de inviolabilidade das comunicações e autodeterminação informativa.

Francesca Bria (2017) se alinha à proposta de Levi ao considerar que a *soberania de dados* pode ser definida como *"o poder que uma comunidade, coletivo ou indivíduo tem de exercer o controle sobre a conversão de suas ações em informações, bem como de autorizar ou não o processamento, cruzamento, armazenamento e utilização desses dados".*

Em outro artigo, este dirigido ao público europeu, Bria (2020) defende que há uma oportunidade para a Europa propor um modelo de economia digital que seja mais sustentável, mais democrático e mais centrado no ser humano. Os europeus poderiam se afastar da visão extrativista e monopolista do capitalismo digital norte-americano, bem como do modelo autoritário de capitalismo chinês.

Um dos trabalhos mais densos sobre soberania no mundo digital é o livro *The Stack* | *On software and Sovereignty* (2015), de Benjamin H. Bratton. Nele, o autor debate como a geografia política agora está vinculada à computação em escala planetária. Este fenômeno implode a lógica da soberania criada no modelo de Vestfália. Sua proposição compromete a existência de uma dinâmica que já ocorre há mais de 300 anos. Apesar de a soberania estatal continuar existindo, ela concorre com espaços multicamadas, como *software*, *hardware* e redes de conectividade, o que nos força a pensar em subdivisões alternativas ao funcionamento da tradicional geografia política.

De uma perspectiva do ordenamento legal brasileiro, Polido (2024) explica que a *soberania digital* é um atributo recente relacionado à autoridade de um ator estatal, seu direito e sua capacidade de controlar dados pessoais e não pessoais, informações e conteúdos no ambiente digital, inclusive as infraestruturas necessárias para seu funcionamento. Na opinião do autor, no que se refere à transferência de dados, a soberania é perdida quando essas informações são enviadas ou compartilhadas com empresas sediadas em um Estado nacional diferente daquele que originou o dado produzido. A jurisdição sobre aquele dado passa a ser do Estado receptor, ainda que esteja armazenado por empresa privada, pois esta está submetida à legislação nacional do local onde está fisicamente alocada. Para Polido, a solução seria fortalecer as instituições da governança global

para uma ordem jurídica transnacional para o ciberespaço, que esteja refletida nas legislações nacionais.

Perder a *soberania digital* traz riscos concretos para os Estados. Desde os atentados terroristas de 11 de setembro de 2001, quando a rede Al-Qaeda promoveu ataques a Nova Iorque e a Washington, o governo dos Estados Unidos vem ampliando sua capacidade de capturar dados para fins de vigilância contra inimigos externos. De acordo com Vanian (2021), mesmo após 20 anos dos ataques terroristas, os cidadãos norte-americanos seguem sofrendo com as repercussões, em especial quanto à sua privacidade *online*. Novas leis foram aprovadas, como a *Patriot Act* (2001), que ampliaram o poder de vigilância das autoridades nos Estados Unidos, principalmente quanto ao monitoramento das comunicações entre indivíduos, em especial os estrangeiros. O pretexto era prevenir e impedir novos ataques de extremistas.

Ao mesmo tempo em que os mecanismos antiterrorismo eram implementados, empresas como Google e Facebook ampliavam suas capacidades de capturar e armazenar dados em razão de seus próprios modelos de negócios. Dentre as leis criadas para regulamentar como o governo dos EUA poderia acessar legalmente as informações capturadas pelas corporações está a “Lei dos Grampos”, ou “Lei de Auxílio das Comunicações para a aplicação do Direito” (USA CALEA Act, 1994). Inicialmente criada para a telefonia convencional, a CALEA foi alterada em 2005 para permitir o monitoramento de Voz sobre IP (VoIP) e de banda larga.

Quando tratamos de *soberania digital*, a CALEA é um elemento-chave. Essa lei obriga que as empresas de tecnologia, inclusive as de *hardware*, tenham *backdoors* em seus dispositivos. *Backdoor* (porta de saída) é uma vulnerabilidade técnica que permite intrusão, quebra de autenticação ou de criptografia.

Com o advento da Computação em Nuvem, o governo norte-americano aprovou a *Cloud Act* (2018), uma lei que permite que autoridades obtenham dados armazenados por empresas de tecnologia, independentemente de estarem localizados em território nacional ou estrangeiro.

Voltando a Vanian, seu artigo relembra o caso de Edward Snowden, que, em 2013, vazou documentos confidenciais que provavam como a Agência de Segurança Nacional (NSA) dos EUA espionava milhares de pessoas, confirmando com

evidências o que antes era somente temor. Até mesmo a Presidenta Dilma Rousseff e a empresa estatal Petrobras foram alvo dos espiões, causando constrangimento diplomático entre Brasil e EUA. Snowden confirmou que a NSA acessava *backbones* da Internet de maneira muito mais habitual do que se imaginava.

Vanian também nos recorda do escândalo da Cambridge Analytica, em 2018, quando dados obtidos de maneira irregular de 87 milhões de clientes do Facebook foram vendidos para uma consultoria que atuava no meio político. Tais informações foram usadas para influenciar o voto popular tanto na campanha presidencial de Donald Trump, em 2016, quanto no referendo do Brexit, que retirou o Reino Unido da União Europeia.

2.4. Faça o que eu digo, não faça o que eu faço

Se os Estados Unidos utilizam suas leis e suas megacorporações para espionar cidadãos e nações estrangeiras, também adotam medidas para impedir que o mesmo ocorra contra sua *soberania digital*. Desde o primeiro mandato de Donald Trump como presidente, os EUA têm boicotado as duas principais empresas chinesas de telecomunicações: Huawei e ZTE (BLOOMBERG NEWS, 2019). Uma das razões é a guerra econômica entre as duas potências, mas um dos argumentos para a inclusão da Huawei na lista de empresas proibidas de comprar de fornecedores norte-americanos é a segurança nacional. O governo Trump também proibiu a empresa chinesa de comprar insumos de companhias dos EUA. Washington passou a exigir que seus aliados rompessem com as corporações chinesas, em especial o *“Five Eyes”*, grupo de cooperação e troca de informações de espionagem, formado por EUA, Reino Unido, Canadá, Austrália e Nova Zelândia.

Em 2021, já com o democrata Joe Biden na Casa Branca, a Comissão Federal de Comunicações (FCC) aprovou um programa de US$ 1,9 bilhão para substituir equipamentos de telecomunicações de empresas chinesas, como Huawei e ZTE, na infraestrutura de redes dos EUA (G1, 2021). No ano seguinte, a FCC proibiu expressamente autorizações para equipamentos chineses de telecomunicações e de vigilância por vídeo, por serem considerados uma ameaça à segurança nacional (FCC NEWS, 2022).

Além das empresas do setor de telecomunicações, os EUA também agiram contra o TikTok, a principal rede social chinesa no Ocidente. Em 24 de abril de 2024, o presidente Biden sancionou uma lei que baniu o TikTok (SAMPAIO, 2024). No entanto, a empresa chinesa teria um prazo para vender a propriedade para um comprador norte-americano, evitando assim a necessidade de simplesmente descontinuar a plataforma para seus 170 milhões de usuários no país.

Em fevereiro de 2024, Biden ordenou uma investigação para saber se veículos chineses conectados à Internet, dotados de *softwares* e componentes produzidos pelo gigante oriental, representariam um risco à segurança dos EUA (FINANCIAL TIMES, 2024). Como no caso das empresas de telecomunicações, fica difícil separar o que é precaução contra a quebra de soberania do que é protecionismo comercial disfarçado. Na verdade, são as duas coisas.

O setor chinês de semicondutores é outro alvo da Casa Branca. Em junho de 2024, os Estados Unidos ampliaram sanções à venda de semicondutores para a Rússia, como um esforço para prejudicar a máquina militar de Moscou em sua guerra contra a Ucrânia. Empresas chinesas que vendem esses dispositivos para a Federação Russa também foram sancionadas (MOHAMMED; LAWDER; FREIFELD, 2024). Em novembro do mesmo ano, os EUA anunciaram que imporiam restrições a *chips* na China que fossem fabricados para fins diferentes dos objetivos para os quais haviam sido inicialmente projetados (HAWKINS, M.; BLOOMBERG, 2024). A medida é vista por Pequim como uma tentativa de frear o avanço tecnológico da nação asiática no campo da Inteligência Artificial. Ao menos 200 empresas chinesas corriam o risco de serem incluídas em uma lista de proibição de comercialização com fornecedores norte-americanos (REUTERS, 2024a).

Adão Villaverde (2024) explica que a produção de dispositivos semicondutores na geopolítica mundial tornou-se fundamental tanto do ponto de vista dos negócios quanto da soberania científica e técnica, sendo estratégica para a segurança das nações. Segundo o autor, os Estados Unidos reservam no seu orçamento público US$ 280 bilhões para os *chips* até 2030. A China, em resposta às restrições, se contrapõe com projeções de US$ 1,4 trilhão, cinco vezes mais.

2.5. Quebrando todas as regras

Não há limites para as agências de inteligência quando os Estados se sentem ameaçados ou decidem perpetrar guerras contra seus inimigos. Desde outubro de 2023, Israel e Hezbollah trocaram ataques de foguetes e projéteis de artilharia. A partir de setembro de 2024, houve uma escalada no conflito, com Israel bombardeando e até invadindo território libanês. Porém, o que chamou a atenção mundial foram as ações de 17 e 18 de setembro, quando dispositivos eletrônicos em posse de militantes do Hezbollah explodiram, matando ao menos 37 e ferindo cerca de 3.400 pessoas. Para evitar rastreamento e vigilância inimiga, o partido islâmico comunicava-se com equipamentos de tecnologia antiga, mais precisamente *pagers* e *walkie-talkies*, uma vez que *smartphones* modernos são mais fáceis de interceptar. De uma maneira ainda não totalmente explicada, um sinal de detonação foi enviado para os equipamentos todos de uma vez, supostamente emitido por Israel, gerando pânico e comprometendo a capacidade de reação. Tel Aviv permitiu que os aparelhos fossem fabricados e, em algum momento antes da entrega, conseguiu com que seus agentes interceptassem e adulterassem milhares de dispositivos, implantando explosivos indetectáveis. Os equipamentos foram entregues e distribuídos pelo Hezbollah à sua militância. Eles permaneceram com os dispositivos durante meses, em plena operação de comunicação, até que, no momento exato, todos explodiram de uma vez (O GLOBO, 2024b).

O caso dos *pagers* pode ser considerado espetacular e extremo, mas as agências de espionagem vêm utilizando os meios eletrônicos e digitais para vigilância há muito tempo. Galloway (2004, p. 25), há mais de duas décadas, já demonstrava como a estrutura da Internet, apesar de ser uma arquitetura distribuída e descentralizada, tinha seus protocolos como severos mecanismos de controle. Apesar de parecer caótica, a rede é regida por hierarquias rígidas de protocolos. Isso permitiu que a Internet se tornasse uma rede global de controle jamais vista.

Em 2001, o Presidente George W. Bush criou, após os eventos de 11 de setembro, um programa contra o terrorismo que recebeu o codinome Stellar Wind. Consistia em obter informações de telefonia e de Internet, incluindo metadados e bancos de dados (THE GUARDIAN, 2013).

Posteriormente, o Stellar Wind foi substituído pelo Projeto PRISM. Com esse novo programa, ao menos desde 2007, a NSA estava obtendo dados diretamente de sistemas do Google, Facebook, Apple e de outras empresas de Internet norte-americanas (GREENWALD; MACASKILL, 2013). Documentos altamente confidenciais foram vazados por Edward Snowden, que mostravam como a agência capturava histórico de buscas em navegadores, conteúdos de *e-mails*, arquivos transferidos e conversas em *chats*.

Quatro anos depois, o WikiLeaks vazou mais de 9 mil documentos, dentre os quais mostravam como a Agência Central de Inteligência (CIA) dos EUA usava técnicas para acessar dados de companhias de tecnologia (COLLINS, 2017). A CIA invadia e acessava produtos eletrônicos e informáticos de uso comum. Em seus manuais havia instruções técnicas para os espiões sobre como atacar um sistema Microsoft Windows ou como transformar uma TV Samsung em um dispositivo de escuta, por exemplo.

Aparentemente, a situação e a imagem dos serviços de inteligência não mudaram com o tempo. Em junho de 2024, a Microsoft admitiu não poder garantir soberania na proteção de dados de policiais e do sistema de justiça criminal escocês hospedados em sua infraestrutura de nuvem pública de hiperescala. A empresa também afirmou que não pode assegurar que os dados sob sua guarda não saiam do Reino Unido (SKELTON, 2024).

Cientistas da Sociedade Alemã de Informática protestaram contra um acordo de cooperação entre o Google e o Escritório Federal Alemão de Segurança da Informação (BSI), em março de 2025, para a criação e desenvolvimento de nuvens seguras e soberanas para autoridades públicas (KREMPL, 2025). Segundo os cientistas, o acordo gera problemas significativos para a segurança, política econômica, concorrência e proteção de dados. O acordo ainda ampliaria a dependência digital alemã e fortaleceria as possibilidades de chantagem por parte dos EUA. Os especialistas apontam que o próprio modelo de negócios do Google é baseado em coleta, análise e uso de dados de terceiros.

Em Portugal, políticos e ativistas propuseram a criação de uma agência de *soberania digital* portuguesa, com o objetivo de enfrentar o que chamaram de “tecnomilionários” e garantir que o país seja autônomo nas infraestruturas de

Internet, evitando a dependência das grandes empresas tecnológicas como a Amazon ou a Google (ESQUERDA.NET, 2025).

Várias empresas europeias estão planejando abandonar as nuvens norte-americanas, temendo riscos de segurança cuja origem é os Estados Unidos. Clientes europeus, especialmente na Dinamarca, estão procurando alternativas para sair das nuvens de hiperescala de empresas norte-americanas após as ameaças diretas e reiteradas de Trump de invadir e anexar a Groenlândia (BURGESS, 2025).

Uma carta com mais de 100 empresas e instituições signatárias defendendo a Iniciativa EuroStack foi endereçada a Ursula von der Leyen, Presidente da Comissão Europeia. O título do documento é *Open Letter: European Industry Calls for Strong Commitment to Sovereign Digital Infrastructure*[3] (EUROSTACK, 2025). Afirmando ser hora para uma ação radical, a carta pede um esforço europeu para tornar a infraestrutura do bloco mais tecnologicamente independente em todas as camadas críticas da infraestrutura digital, seja na infraestrutura lógica (aplicações, plataformas, mídia, *frameworks* e modelos de Inteligência Artificial) ou na infraestrutura física (*chips*, processamento, armazenamento e conectividade). Para as signatárias, atualmente há múltiplas dependências que criam riscos de segurança e confiabilidade, que comprometem a soberania europeia e prejudicam o crescimento econômico. A Iniciativa EuroStack é uma proposta de política industrial que reúne tecnologia, governança e financiamento para infraestruturas digitais.

A China acusou os EUA de espionagem em escala global por meio de dispositivos móveis e operadoras de telecomunicação. A denúncia tem base em um relatório da Aliança Chinesa da Indústria de Segurança Cibernética. Segundo o documento, funcionários do governo chinês, especialistas técnicos e pessoas comuns poderiam ser alvo dos serviços de inteligência norte-americanos. Dentre as táticas utilizadas pelos agentes dos EUA estão ataques a SIM Cards e às redes móveis de telefonia celular, exploração de falhas em iPhones, uso de *spywares* comerciais, uso de estações falsas de comunicação para interceptação de chamadas, infiltração em operadoras de telecomunicação e coleta de dados via aplicativos pré-instalados (VIDAL, 2025).

---

3 TRADUÇÃO LIVRE: *"Carta Aberta: Indústria Europeia pede forte compromisso com infraestrutura digital soberana"*

2.6. Soberania à venda … mas quem está comprando?

A preocupação com *soberania digital* na China já ocorre há muitos anos. Em 2010, a China já havia forçado o Google a encerrar suas operações no país. Divulgada no Ocidente como uma queda de braço entre uma ditadura e uma empresa defensora da liberdade de expressão (SALATIEL, 2025), o conflito revelaria a dificuldade da corporação em respeitar determinações do governo chinês. Gostasse ou não do que lhe estava sendo pedido, o Google tinha obrigação de cumprir as determinações do poder local, o que teve muita dificuldade em fazer.

Em 2021, o país asiático aprovou uma nova regulamentação sobre defesa e segurança de dados, que não poupou nem mesmo as grandes corporações de Internet daquela nação. As chinesas Alibaba, Tencent, DiDi e Baidu, por causa da nova lei, chegaram a perder valor de mercado em bolsas de valores pelo mundo de 30% a 45% (CAUTI, 2021).

E em outros mercados, como o brasileiro? Atentas à pressão decorrente do debate sobre a *soberania de dados*, as *Big Techs* ocidentais colocaram seus departamentos de *marketing* para trabalhar. Quase todas as grandes empresas de TICs empacotaram seus produtos e serviços e os venderam como solução. Quer soberania? É só comprar.

Uma das primeiras empresas a adotar essa prática foi a Oracle. Governos e empresas que têm preocupações com localização de dados, acesso e controles operacionais podem contratar a Oracle Cloud Infrastructure (OCI) e o problema estará resolvido, segundo as propagandas da corporação. Conforme o portal Oracle.com, a empresa promete atender às necessidades de conformidade, legais e regulatórias, assim como dar capacidade de auditoria sobre os sistemas de TI, além de restringir o acesso aos fluxos de dados e informações operacionais. Com isso, seus clientes teriam os benefícios de uma nuvem distribuída, sem perda de decisões soberanas, sem gastos adicionais e sem perder o que há de melhor na tecnologia (ORACLE, 2025). Como argumentos de vendas, tais promessas são imbatíveis.

A Microsoft oferece o produto Microsoft Cloud for Sovereignty, que, segundo a empresa, torna a plataforma de nuvem Azure compatível com exigências dos poderes locais e permite mitigar riscos de soberania. Dentre os recursos disponíveis,

há computação confidencial, segurança de *hardware* gerenciado, transparência das atividades do operador da nuvem e políticas de conformidade regulatória, dentre outras funcionalidades (MICROSOFT, 2025a).

A nuvem Amazon Web Services (AWS) também se compromete a garantir autonomia digital por meio de *design* de produtos. A empresa promete desenvolvimento contínuo de funcionalidades para controle e para atendimento de requisitos regulatórios. Afirma investir em mecanismos de localização de dados do cliente, com controles verificáveis sobre o acesso, com limites de segurança física e lógica que impediriam até seus funcionários de acessar cargas dos contratantes sem autorização, e também na capacidade de criptografar qualquer dado em qualquer lugar (AWS, 2025).

A Google Sovereign Cloud segue a mesma linha de seus concorrentes. Divide seu produto de soberania em três pilares: *soberania de dados*, Soberania Operacional e Soberania de *software*. O primeiro pilar é o controle sobre criptografia e acesso a dados. O segundo refere-se à capacidade de rodar cargas de trabalho sem depender de provedores de *software*. O terceiro trata da visibilidade e controle sobre as operações do provedor de serviços (GOOGLE, 2025).

Segundo o *marketing* das empresas, depender das *Big Techs* para ter *soberania de dados* deixa de ser um problema e passa a ser uma solução de mercado. Passa-se a observar a concorrência, avaliando quem oferece o melhor serviço de localização de dados e infraestrutura, controle de hospedagem, restrição de acessos, escolha de nuvens separadas para diferentes usos, suporte a operações locais e segurança sobre criptografia.

É preciso notar que a própria oferta desses serviços já denuncia a fragilidade do sistema. Se é possível o provedor de serviços realizar todas essas operações, significa que ele tem poder tecnológico para também não as cumprir, se necessário for. Ao contratar serviços de nuvens soberanas das *Big Techs*, os governos-clientes continuam a ter seus dados sob o poder das grandes corporações. A empresa que controla a tecnologia pode, a qualquer momento, por qualquer razão, romper com os contratos estabelecidos, mesmo que ilegalmente, e capturar os dados que precisar sequestrar. Pode também criar formas de bloquear o acesso à tecnologia, tornando inviável a sua utilização.

Consultores empresariais costumam responder a esse tipo de risco como sendo algo improvável, pois as corporações teriam danos de credibilidade e de imagem, comprometendo contratos com outros clientes. No entanto, isso é facilmente refutável por duas razões. Primeiro, toda ou parte significativa das tecnologias vendidas como produtos ou como serviços pelas *Big Techs* são opacas, verdadeiras caixas-pretas, que não permitem ou dificultam ao cliente saber o que estão processando, como estão verdadeiramente funcionando. A segunda razão é que, dependendo do interesse geopolítico em jogo, o que seria uma quebra de contrato com uma empresa de um país periférico? Mais do que isso, as *Big Techs* precisam cumprir leis e decisões judiciais oriundas de suas matrizes, o que lhes daria álibis junto aos demais clientes. A entrega de dados sigilosos para autoridades seria forçada por decisões de magistrados.

As duas maiores estatais do Governo Federal do Brasil, Serpro e Dataprev, estão seguindo o caminho indicado pelas multinacionais norte-americanas. As estatais federais anunciaram a construção de uma “nuvem 100% soberana” (SERPRO, 2024a; BRASIL, 2024b), em parceria com as *Big Techs*. As empresas-clientes dizem que se importam com soberania, mas parecem desconhecer a famigerada *Cloud Act* (2018). Apenas essa lei já seria suficiente para rever toda e qualquer política nacional de segurança de dados em países periféricos.

A Divisão Criminal do Departamento de Justiça dos EUA explica que a *Cloud Act* foi elaborada para, dentre outros objetivos, acelerar o acesso à informação eletrônica armazenada por provedores globais com base nos Estados Unidos. Terrorismo, exploração sexual de crianças e crimes cibernéticos estão entre os elementos que podem motivar investigação de conteúdos. A lei, em seu § 2713, deixa claro que dados de clientes devem ser preservados e, dentro dos termos legais, devem ser divulgados obrigatoriamente para as autoridades, se solicitado conforme regulamento. Estão sujeitas a monitoramento as comunicações eletrônicas ou por fio, todos os tipos de registro, cópias de segurança ou quaisquer informações pertencentes a um cliente ou assinante, que estiverem sob controle do provedor, dentro ou fora dos Estados Unidos (USA, 2023a).

O Departamento de Justiça afirma que requisições de evidências eletrônicas são frequentemente demandadas por autoridades estrangeiras e, por isso, é preciso

trabalhar em assistência legal mútua. A *Cloud Act* também foi pensado para permitir aos governos estrangeiros proteção de privacidade e liberdades civis em seus próprios países.

O Brasil mantém um acordo de assistência judiciária com o governo norte-americano, chamado *Mutual Legal Assistance Treaty* (MLAT), que segue em vigor (BRASIL, 2019a). Foi promulgado pelo Decreto nº 3.810/2001 da Presidência da República (BRASIL, 2021), que, dentre os pontos de assistência, inclui o fornecimento de documentos, registros e bens, além da localização ou identificação de pessoas (físicas ou jurídicas). O decreto reserva a cada um dos países o direito de negar a assistência e a troca de informações.

O problema é que a relação entre os EUA e outras nações é assimétrica. Enquanto os Estados Unidos podem obrigar suas empresas a entregarem dados, os governos estrangeiros têm limites claros quanto à imposição do cumprimento das leis locais às *Big Techs* norte-americanas.

Sérgio Rosa, que foi diretor do Departamento de Informação e Informática do Sistema Único de Saúde (DATASUS), subordinado ao Ministério da Saúde do Brasil, concedeu entrevista para Joyce Ariane de Souza, na qual esclarece sua visão sobre qual deveria ser a postura de gestores preocupados com a *soberania de dados*:

> *Estando na Amazon tem mais facilidade de uso. Mas eu não preciso ter tanta facilidade e colocar os dados dos cidadãos em risco. Vai perder eficiência, vai ser um pouco mais lento, não vai ter relatórios de BIA maravilhosos, não, não vai, mas o principal é o dado do cidadão e ele deve estar nas infraestruturas e tecnologias nacionais. Esse é um conflito que a gente vive, eu não paro de receber a Microsoft, a Amazon, a Huawei. Todo mundo vai lá falar. Até a Embratel. Todos têm soluções maravilhosas e a pressão é grande, porque são os lobbies com grande poder de dinheiro e político. Então já chegam com a coisa quase que feita e a gente tem que dizer, calma, vamos devagar, vamos fazer um levantamento primeiro, vamos estudar as soluções.* (ROSA, 2023, p. 201)

Mas por quais motivos os Estados Unidos usariam suas corporações de Tecnologia da Informação para atacarem o Brasil, um aliado histórico? Seria uma hipótese remota? Nem tanto. Já comentamos sobre como Snowden denunciou a espionagem norte-americana contra Dilma Rousseff e a Petrobras, em 2013. Outros fatos mais recentes também exigem estado de atenção do governo brasileiro.

Em 2024, a empresa X (ex-Twitter), de Elon Musk, desafiou o Supremo Tribunal Federal do Brasil ao tentar não cumprir obrigações legais (REUTERS, 2024b). Depois, em fevereiro de 2025, a Câmara dos EUA aprovou um projeto que foi chamado pela imprensa brasileira de “Lei anti-Moraes”, cujo texto legal visa impedir autoridades estrangeiras acusadas de promover censura a qualquer cidadão dos Estados Unidos, em solo americano, tendo como alvo o Ministro do STF, Alexandre de Moraes, visto como um vilão pela extrema direita (GATTO, 2025).

Em abril do mesmo ano, às vésperas de aumentar tarifas de importação para produtos de vários países, foi divulgado um relatório do Governo dos EUA que serviu como base para justificar as tarifas regulatórias contra o Brasil (GROSSMANN, 2025a). Dentre os pontos apresentados, além de *commodities*, como álcool e carnes, o documento cita expressamente as regulações brasileiras em setores estratégicos, como telecomunicações (que dificultam a ampliação da rede Starlink no Brasil), a Lei Geral de Proteção de Dados (Lei 13.709/18) e possibilidades de taxação das *Big Techs* pela Anatel.

CAPÍTULO 3
DO FATIAMENTO DA SOBERANIA

O objetivo deste capítulo é demonstrar como ocorre o fatiamento da soberania e da capacidade de intervenção do Estado no ambiente digital. Como afirmara Michael Kwet, o controle das infraestruturas, sejam elas físicas ou lógicas, é o que confere poder para ditar os rumos no ambiente virtual. São cadeias complexas, que envolvem empresas de diversos segmentos de mercado, espalhadas pelo mundo. Os arranjos que permitem à Internet e à Inteligência Artificial funcionarem dependem de uma variedade enorme de atores, cada um com suas próprias características.

Numa época em que a Internet ainda não estava disseminada pelo planeta, Susan Strange, no livro *States and Markets* (1988), já propunha uma divisão da estrutura da economia mundial em quatro partes: 1) estrutura de segurança; 2) estrutura de produção; 3) estrutura financeira; e 4) estrutura do conhecimento. Em sequência, haveriam outras quatro estruturas de poder secundárias: 1) sistemas de transporte (naval e aéreo); 2) comércio; 3) energia; e 4) bem-estar (benefícios e oportunidades de um povo, incluindo políticas públicas). Strange já demonstrava como essas estruturas de poder se configuravam de maneira complementar. Para a autora, o poder não é exercido apenas por meio da força e da lei, mas também pela criação de estruturas que moldem pessoas, corporações e estados, influenciando suas burocracias, atividades comerciais, tecnologias e as relações entre elas.

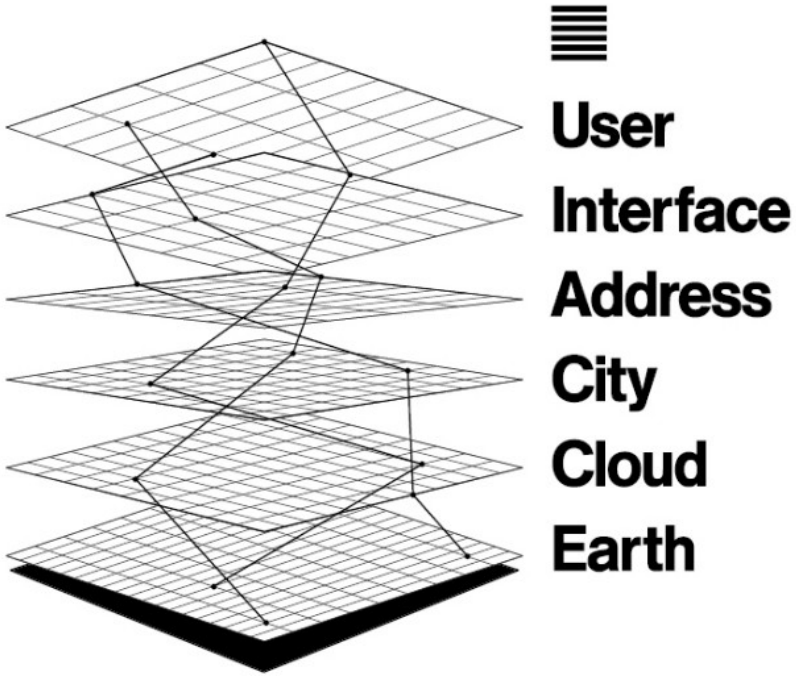
Seguindo uma lógica semelhante à de Strange, já no século XXI, Benjamin Bratton (2015) propõe um olhar para a realidade por meio do estabelecimento de camadas, nas quais ocorre o fatiamento da soberania. Bratton denomina esse modelo de organização como *The Stack* (algo como *“A Pilha”*, em português). Para o autor, o modelo de geografia geométrica não funciona mais, assim como o sistema de soberania criado com a Paz de Vestfália, que está ultrapassado.

The Stack seria uma megaestrutura acidental, cuja existência não foi concebida de maneira centralizada para que fosse como é. Não houve um plano mestre, nenhum líder, nenhum evento revolucionário. Ela simplesmente foi se formando. A era da computação em escala planetária, na expressão criada por

Bratton, não elimina as estruturas verticais que precedem o mundo digital. Ele as separa em *geografias seculares emergentes* (como a computação em nuvem ou interfaces de computador) e *geografias sacras e arcaicas* (como o totalitarismo religioso). Ambas competem entre si, mas também colaboram entre elas. Um exemplo é o uso de aparelhos celulares com conexão satelital para detonar explosivos em ataques terroristas suicidas. Poderíamos incluir aqui o uso de redes sociais em campanhas de desinformação antivacinação.

Na substituição ao modelo de Vestfália, o sistema técnico e geopolítico *The Stack* seria composto por seis camadas independentes, que variam em escala e se complementam: a *Terra*, a *Nuvem*, a *Cidade*, o *Endereço*, a *Interface* e o *Usuário*. Formam um sistema multicamada, que interage de maneira modular e interdependente, combinando estruturas computacionais e não computacionais. A Figura 3 demonstra como as camadas estariam sobrepostas.

Figura 3 – The Stack – Diagrama de Metahaven.



Fonte: BRATTON, 2015, p. 108

Cada camada tem sua característica e um papel específico no modelo. O *Usuário* é o sujeito da ação, que aciona as interfaces computacionais, permitindo a manipulação de elementos alocados em *Endereços* que ocupam espaços no ar, no mar ou na terra. Os endereços localizados na superfície urbana pertencem à camada da *Cidade*. Já o processamento, o armazenamento de dados e a capacidade computacional residem na camada da *Nuvem*. Por fim, temos a camada do planeta *Terra*, de onde extraímos a energia para alimentar os *data centers* e os minérios, como silício, cobre ou alumínio, para produzir os *hardwares* dos computadores e demais equipamentos.

Recortar a realidade em camadas, como fez Benjamin Bratton, é uma abstração interessante, mas arbitrária. Não é a única forma de dividir a *soberania digital*. BELLI (2023), por exemplo, apresenta seus próprios habilitadores-chave para a soberania em Inteligência Artificial: *Key AI Sovereignty Enablers* (KASE). A segmentação de Belli possui oito partes: 1) governança de dados; 2) governança algorítmica; 3) capacidade computacional; 4) conectividade significativa; 5) energia elétrica confiável; 6) alfabetização digital da população; 7) segurança cibernética robusta; e 8) arcabouço regulatório apropriado.

Qual segmentação está correta? A de Bratton ou a de Belli? Não há certo e nem errado. Cada autor fez sua divisão conforme o método que gostaria de usar em suas análises. O que chama atenção é que se tentarmos sobrepor uma divisão à outra, haverá certa dificuldade.

3.1. Subdivisões na camada de Nuvem

Rodolfo da Silva Avelino (2021) apresenta a descrição das camadas TCP/IP, conjunto de protocolos de comunicação da Internet, que é um sistema interconectado de redes heterogêneas e distintas. Esse sistema envolve elementos diversos, como computadores, dispositivos, roteadores (*hardwares*), números de redes IP e a comunicação de dados lógicos por meio de protocolos técnicos (*Ibid*., p. 39). Na subdivisão, a Internet possui quatro camadas: 1) aplicação; 2) transporte; 3) rede; e 4) acesso à rede. A Figura 4 detalha cada uma delas.

Figura 4 - Descrição das camadas TCP/IP e dos SDOs.

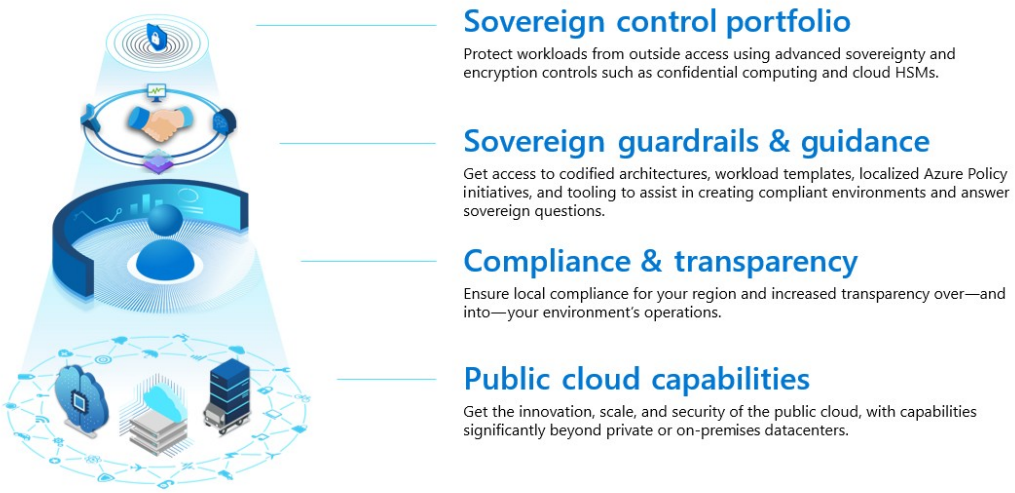
Camada	Descrição	Alguns Protocolos	SDOs
4 – Aplicação	Contém os protocolos que oferecem serviços na Internet, como protocolos de e-mail, mensagem instantânea, páginas de web, entre outros serviços.	HTTP, HTTPS, SMTP, POP, DNS, XMPP E FTP	W3C, OASIS, IETF
3 – Transporte	É responsável por controlar a comunicação entre os computadores, servidores e dispositivos conectados.	TCP e UDP	IETF
2 – Rede	Por meio de algoritmos, traça a melhor rota dinâmica e/ou estática para que os dados de uma comunicação cheguem até o seu destino.	IP	IETF
1 – Acesso à Rede	Acesso à rede (Host/Rede).	Ethernet, wi-fi, fddi	IEEE ETSI

Fonte: Camdas TCP/IP, extraído de AVELINO, 2021, p.41

A Internet vai além de seus aspectos meramente técnicos. Ela envolve fatores políticos, sociais, jurídicos e culturais. A Governança da Internet depende de gestões separadas para conteúdos, lógica e infraestrutura. Para cada um dos elementos envolvidos, ocorrem intensas disputas políticas e econômicas. Cada empresa possui sua linha de produtos e serviços e tenta fazer dos seus ativos o padrão da rede ou, pelo menos, garantir sistemas interoperáveis que não excluam seus produtos. Evitar batalhas de padrões é uma preocupação constante dos que trabalham com governança internacional de TI. Os interesses comerciais buscam influenciar as decisões a todo momento. Não é simples evitar o jogo de hipocrisia que ocorre nos fóruns internacionais. Via de regra, as corporações ou governos alinhados a elas tentam convencer que um determinado padrão ou protocolo (preferencialmente aquele protegido por sua propriedade intelectual) é melhor para todos, ao mesmo tempo em que procuram evitar que o padrão fechado proposto pelo concorrente se torne a regra. O debate sobre interoperabilidade e padrões abertos é o consenso óbvio e possível, mas pode ser comprometido a qualquer momento, ao menor sinal de fraqueza ou vacilação de uma das partes envolvidas.

As corporações também adotam o conceito de camadas no desenvolvimento de seus produtos. Neles, colocam os padrões que mais lhes interessam, algumas vezes sem considerar padrões interoperáveis pactuados internacionalmente. O desenho de *soberania digital* da Microsoft é dividido em controle de portfólio, proteção de dados contra acessos externos, medidas de segurança e orientações de procedimentos, conformidade e transparência, além do desenvolvimento de novas capacidades de segurança para nuvens públicas (MICROSOFT, 2025b). A Figura 5 mostra como são construídas as camadas dentro do Microsoft Cloud for Sovereignty.

Figura 5 – Camadas do Microsoft Cloud for Sovereignty



Fonte: MICROSOFT, 2025b

3.2. Infraestruturas do digital

Nesta tese de doutorado, a proposição de camadas do digital deve levar em consideração a realidade brasileira, suas características e o controle de propriedade sobre cada uma dessas infraestruturas. O processo de enfrentamento da perda de soberania só será possível se o Estado agir sobre elas, recuperando ou criando mais capacidade de ação. Dividiremos as infraestruturas em duas categorias: físicas e lógicas. A infraestrutura física corresponde à parte material, enquanto a infraestrutura lógica é a parte por onde os dados transitam.

As infraestruturas do digital devem ser separadas em:

- Infraestruturas físicas:

1. Energia elétrica;
2. Telecomunicações;
3. *Hardwares* e equipamentos;
4. *Data centers*;

- Infraestruturas lógicas:

5. *Softwares* básicos;
6. Desenvolvimento de sistemas;
7. Bases de dados;
8. Inteligência Artificial.

3.2.1. Energia elétrica

A produção de energia, sem dúvidas, é o maior problema geopolítico e ambiental. Não são por acaso as constantes guerras no Oriente Médio e as tensões internacionais por petróleo, que ainda é a principal fonte de energia. A queima de combustíveis fósseis representa 87% das emissões globais de CO^2, segundo relatório da IEA de 2022. Quem é leigo no assunto pode pensar que o mundo digital é uma solução para colaborar com a redução da poluição, uma vez que o digital é intangível e ocorre apenas no virtual. Nada poderia estar mais distante da realidade. A chamada *transformação digital* da sociedade exige uma infraestrutura tecnológica que consome quantidades alarmantes de energia, e toda a perspectiva aponta para um aumento no consumo. Segundo dados do Fórum Econômico Mundial, os *data centers* são responsáveis por 2,5% de todo o dióxido de carbono produzido pela humanidade, um valor superior ao emitido pela indústria da aviação, que é 2,1% (UM SÓ PLANETA, 2023).

Poderia se argumentar que a energia é uma externalidade para o funcionamento das infraestruturas do digital. As razões para esse pensamento são que, como considerou Strange (1988), a energia é uma estrutura de poder secundária. Depois, pelo fato de que a eletricidade é necessária a praticamente todas as atividades avançadas no mundo pós-industrial. Porém, como defendeu Boutang (2007b), em seu *capitalismo cognitivo*, as externalidades não são mais marginais.

Imagine um mundo sem eletricidade. Outras indústrias poderiam sofrer adaptações, recorrer a métodos antigos e retomar a produção de maneira artesanal. Na produção de alimentos, ainda que a queda de produtividade levasse a uma grande fome, o setor encontraria uma forma de se reorganizar, com o retorno dos camponeses como principal fonte da produção. O mesmo valeria para a indústria bélica. Em caso de guerra, a falta de acesso a recursos para fabricação de armas e munições faria com que a criatividade atuasse para desenvolver alternativas e manter o esforço de combate. Flechas seriam fabricadas com estiletes.

No mundo digital, nada disso é possível. A ausência de energia elétrica significa, simplesmente, a abolição do virtual. Por tal razão, a energia é uma infraestrutura obrigatória, que deve ser observada também nos estudos de *soberania digital*. Nessa infraestrutura estão as linhas de transmissão, as usinas hidrelétricas, térmicas, nucleares, solares, eólicas ou de qualquer outro tipo, as subestações e as conversoras.

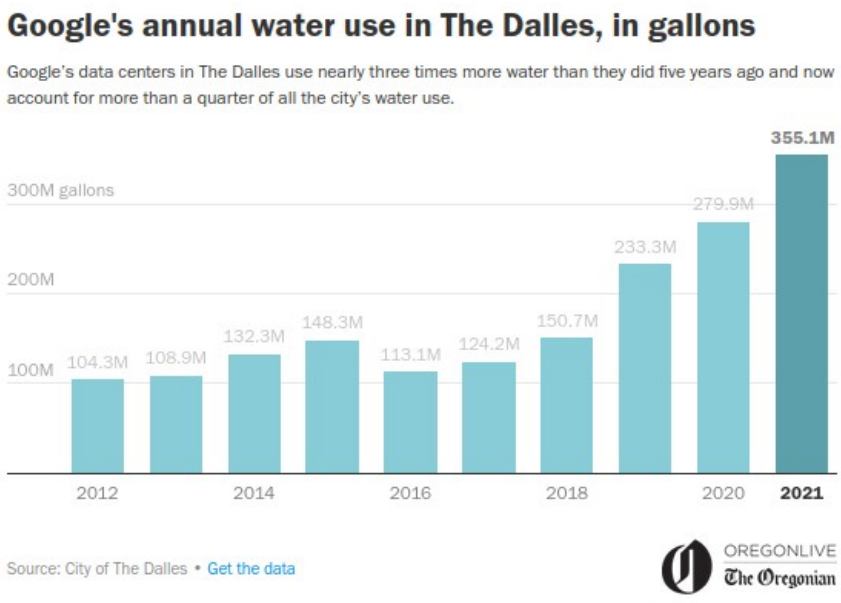
Em setembro de 2024, a Microsoft anunciou a intenção de reabrir uma usina nuclear na Pennsylvania, EUA, até 2028. A usina Three Mile Island está fechada desde 1979, quando ocorreu um grave acidente no local (SHERMAN, 2024). Um mês depois, foi noticiado que o Google planeja construir seus próprios reatores nucleares de pequeno porte para alimentar seus sistemas de Inteligência Artificial. Seriam sete reatores com capacidade de gerar 500 megawatts. O projeto prevê que o primeiro deles comece a operar no ano de 2030 (AL JAZEERA, 2024). Apenas dois dias após a matéria sobre os planos do Google, noticiou-se que a Amazon começaria a investir em energia nuclear para suprir a crescente demanda de seus *data centers*. O investimento inicial previsto é de US$ 500 milhões. O plano é produzir 5 gigawatts até o ano de 2039 (EURONEWS, 2024).

A China teve que restringir a mineração de bitcoins e outras criptomoedas em seu território devido ao consumo excessivo de energia dessas atividades. Começou com governos locais: primeiro na região da Mongólia Interior, depois os governos de Xinjiang, Qinghai, Yunnan e Sichuan decretaram a proibição (EXAME, 2021). Por fim, o governo central decidiu banir a mineração de criptomoedas em toda a China, alegando combate à especulação financeira (REUTERS, 2021).

De acordo com o *Cambridge Bitcoin Electricity Consumption Index* (CCAF, 2025), a mineração de Bitcoin consumiu 144,23 TWh de energia em 2019, enquanto a mineração de ouro consumiu 131 TWh. Cada TWh equivale a um bilhão de kWh (kilowatt-hora). Como comparação, o estado de São Paulo, com cerca de 45,9 milhões de habitantes, em 2019, consumiu 133 TWh (SÃO PAULO, 2019).

O consumo de energia nos *data centers* se dá principalmente pela necessidade de resfriamento. Em The Dalles, EUA, o consumo de água do Google triplicou em cinco anos, entre 2017 e 2022. Mais de um quarto de todo o consumo da água extraída do Rio Columbia estava sendo usado pela gigante de tecnologia, trazendo riscos para peixes e outros animais da fauna local (ROGOWAY, 2022). A Figura 6 traz a evolução do consumo de água em galões.

Figura 6 - Uso anual de água pela Google em The Dalles, em galões.



Fonte: ROGOWAY, 2023

A pegada energética do setor de Tecnologias da Informação, em 2021, foi estimada em 7% do consumo global de eletricidade. Esse número equivale a 160% do consumo do Brasil em um ano (FONSECA; MICHELLIS JR., 2021). No mundo, as TICs gastaram 800 TWh, sendo os *data centers* responsáveis por 320 TWh, a mineração de criptografia por 140 TWh e a transmissão de dados por 340 TWh. O Brasil inteiro consumiu 497 TWh no mesmo período.

Para Fonseca e Michellis, a solução para mitigar o problema de consumo de *data centers* passaria por várias ações, como a melhoria da eficiência energética, o uso de energias renováveis e o desenvolvimento de um *design* eficiente baseado em *software* para que os equipamentos gastem menos energia. A produção de novos *hardwares* precisaria evoluir para um menor consumo no processamento. Outra possibilidade é a construção de edifícios ecológicos. Isso se somaria a um melhor gerenciamento da climatização e dos sistemas de ar-condicionado. Em países de clima frio, o calor gerado pelos *data centers* poderia ser redirecionado para construções vizinhas, sendo aproveitado para calefação.

Como potência na geração de energia renovável e com uma matriz energética limpa, o Brasil poderia apostar em suas capacidades hidrelétrica, fotovoltaica e eólica para instalar *data centers* em solo nacional. Tal medida precisa ser adotada junto com outras ações que garantam que conhecimentos, inteligência e capacidade de desenvolvimento em TICs acompanhem o crescimento no número de *data centers*. Não se pode permitir que o Brasil seja apenas fonte da *commodity* eletricidade e que todo o capital cognitivo fique nas mãos de empresas estrangeiras. Se isso ocorrer, teremos mais uma forma de extração e exportação de matéria-prima, como é feito desde a época do colonialismo histórico. Não é possível ser a base para a economia de dados e ficar apenas com os danos ambientais.

O planejamento para a expansão do setor elétrico deve levar em consideração, além da capacidade de geração de energia, sua infraestrutura de transmissão. O Sistema Integrado Nacional cobre quase todo o território nacional, exceto Boa Vista (RR), que está isolada do sistema devido à limitação geográfica imposta pela floresta Amazônica. Em 2023, havia 172.019,85 km de linhas de transmissão da Rede Básica. A Figura 7 apresenta a distribuição pelo Brasil.

Figura 7 – Sistema Interligado Nacional do Operador Nacional do Sistema, 2023

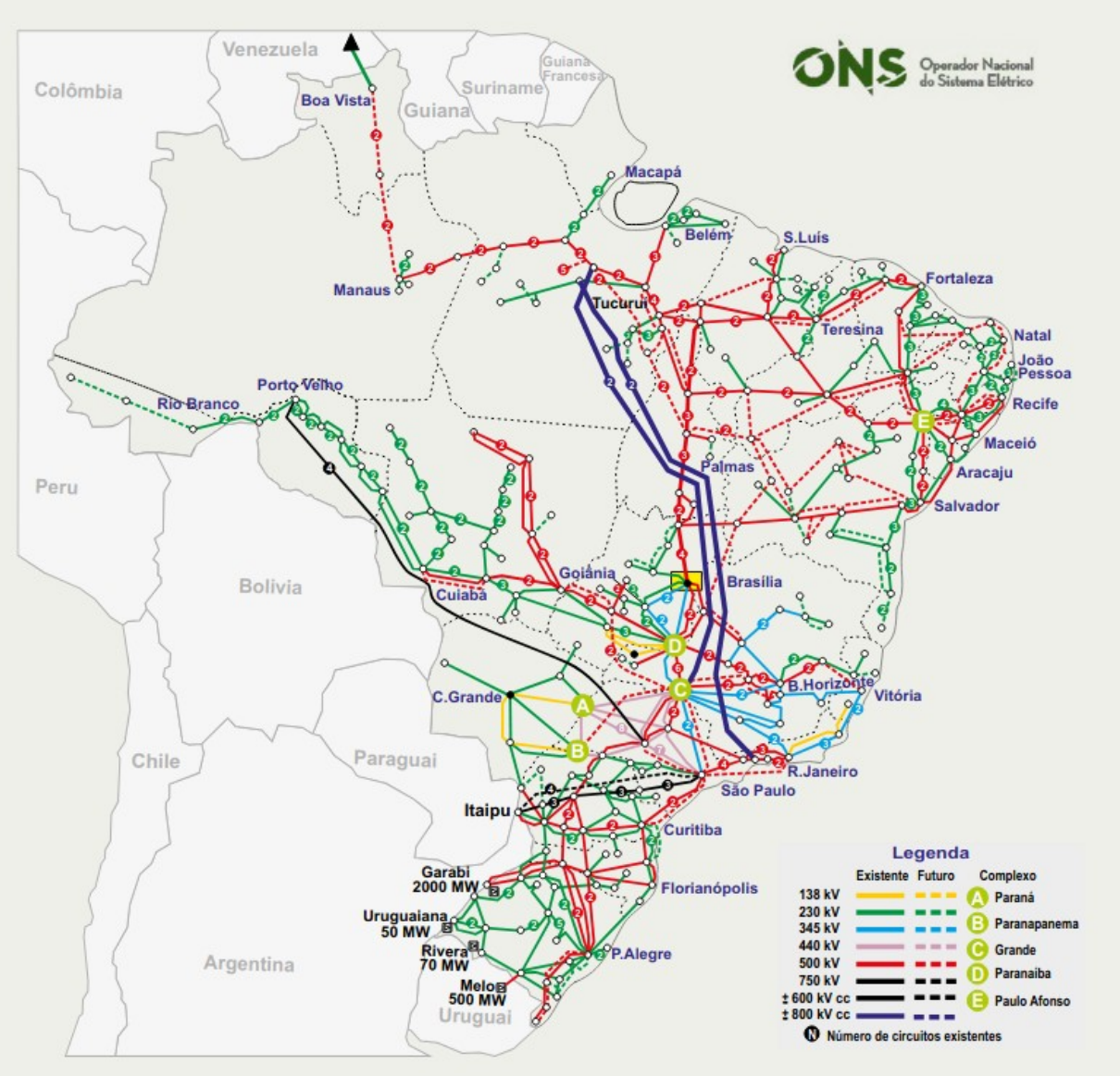


Figura 7: Sistema Interligado Nacional do Operador Nacional do Sistema, 2023

Fonte: BDT. Rede Básica existente em dezembro de 2023. In: Relatório Anual 2023, ONS

A maior parte das linhas de transmissão do Brasil é controlada pelo setor privado. Apesar do agravamento dessa situação a partir da onda de privatizações da década de 1990, a construção da rede de energia no país sempre teve a participação do capital estrangeiro. Farias (2006) faz um breve histórico de como ocorreu esse processo.

Em 1889, houve a inauguração da primeira usina elétrica brasileira pelo Imperador Dom Pedro II. Foram empresas estrangeiras, The São Paulo Railway e a Light and Power Company, que obtiveram as concessões para a distribuição de energia, garantindo-lhes um mercado cativo. O setor evoluiu lentamente. Apenas na década de 1960, com a pressão decorrente do projeto de industrialização e a intensificação da urbanização, surgiu uma forte demanda. O Estado brasileiro passou a ser o indutor dos investimentos. Em 1984, o consórcio Brasil-Paraguai construiu a usina hidrelétrica de Itaipu, que foi a maior do mundo durante muitas décadas. Nos anos noventa, marcados pelo avanço da onda neoliberal na América Latina, começaram a ser alterados os marcos legais para permitir consórcios de concessionários. Nessa fase, empresas como as norte-americanas Enron Corporation e o Grupo AES entraram no mercado brasileiro, com grupos portugueses, espanhóis, franceses, canadenses e belgas (*Ibid.*, p. 102). O Estado brasileiro manteve-se, durante todo o período, financiando, subsidiando e socorrendo as concessões públicas.

Atualmente, há uma forte presença de estatais estrangeiras no controle das concessões elétricas no Brasil. A China, que não participou das aquisições no início do processo de privatização, por meio da estatal State Grid, comanda hoje 24 concessionárias e venceu o maior lote do leilão de energia promovido pelo Governo do Brasil em 2023 (CARNAES, 2024). É curioso que o argumento dos neoliberais para defender as privatizações era a eficiência do setor privado em relação ao setor público. O que aconteceu foi o avanço de estatais estrangeiras em um setor estratégico nacional.

Para acompanhar o modelo de concessionárias, o Estado brasileiro apostou no modelo de agências reguladoras. Criou-se a Agência Nacional de Energia Elétrica (ANEEL), uma autarquia que teria por missão regular e fiscalizar a produção, transmissão, distribuição e comercialização de energia elétrica (FREITAS, 2024). Segundo dados do Portal da Transparência (BRASIL, 2025a), a ANEEL conta com pouco mais de 900 servidores para acompanhar toda a complexidade do sistema elétrico brasileiro. Há sérios limites na capacidade de uma pequena agência para enfrentar o poder de corporações enormes.

Um exemplo claro da deficiência da capacidade de ação do Estado com o modelo de agências reguladoras foi os apagões na cidade de São Paulo, em 2024. A empresa de energia que atende a capital paulista e sua região metropolitana é a Enel, controlada por um grupo italiano. O primeiro apagão ocorreu em novembro de 2023, quando a empresa demorou seis dias para restabelecer plenamente o funcionamento da energia, prejudicando 3,7 milhões de pessoas. O segundo apagão aconteceu em meio a uma campanha eleitoral para eleger os novos prefeitos e vereadores, o que fez do episódio um dos principais temas de debate entre os candidatos. Dessa segunda vez, 2,7 milhões de pessoas foram diretamente afetadas (SOUZA, B.; 2024).

Com medo dos resultados das urnas, a concessionária Enel, a Prefeitura Municipal de São Paulo, o Governo do Estado de São Paulo, o Ministério de Minas e Energia e a ANEEL travaram uma guerra pública de versões, em que cada um buscava transferir para os outros a culpa pela demora na resolução do problema. O episódio atabalhoado foi uma demonstração de que a agência tem pouca vontade ou poder de exigir ações concretas das empresas.

3.2.2. Telecomunicações

O setor de telecomunicações foi a infraestrutura símbolo do processo de privatização no Brasil nos anos 1990. Em quase 30 anos, o segmento viveu mudanças profundas. O serviço de telefonia analógico deixou de ser o principal produto. Em seu lugar, ganharam importância a transmissão de sinal digital, a transferência de dados em alta velocidade via fibra ótica e a telefonia celular. A infraestrutura das redes de telecomunicação são como estradas e rodovias do mundo digital, garantindo conectividade e fluxo acelerado de informações.

Figura 8 – Mapa da Infraestrutura de Conectividade no Brasil, 2025

Fonte: Ahttps://bbmaps.itu.int/bbmaps , 2025

No portal da International Telecommunication Union – ITU (www.itu.int) é possível ter acesso a mapas interativos de infraestrutura de 194 países. Há também dados divulgados por mais de mil empresas, universidades e organizações regionais. Navegar pelos mapas ajuda a compreender a distribuição geoespacial dos cabeamentos das redes digitais. Alguns países sonegam dados, principalmente por razões de segurança, mas o Brasil é considerado um dos que melhor dão transparência de suas informações.

A infraestrutura de telecomunicações depende de postes nas ruas das cidades e, na maioria dos casos, tais postes são compartilhados com o setor de energia elétrica (PISTONO, 2024). Distribuidoras de energia e de telecomunicações são frequentemente aliadas nos debates legislativos sobre ocupação e uso dos postes, sendo que, na maior parte dos casos, a regulação sobre o espaço urbano é responsabilidade de cada município.

A transmissão de dados por antenas também faz parte da infraestrutura de telecomunicações. Atualmente, as tecnologias 2G e 3G estão sendo descontinuadas e suas antenas estão sendo desativadas. Já a tecnologia 4G chega a 93% da população no Brasil, por meio de serviços prestados por sete operadoras. Se considerarmos apenas moradores de áreas urbanas, a cobertura chega a 99,7%. Já em áreas rurais, a cobertura é de 57,69%. Os dados são do *Painel de Dados de Infraestrutura* da Agência Nacional de Telecomunicações (Anatel)[4].

De acordo com o *Infográfico Setorial de Telecomunicações* da Anatel, de março de 2022, o mercado é subdividido em quatro grandes tipos de serviço: 1. telefonia móvel (258,3 milhões de celulares); 2. banda larga fixa (40,8 milhões de pontos de acesso); 3. telefonia fixa (27,9 milhões de telefones fixos); e 4. TV por assinatura (15,6 milhões de assinantes). As empresas Vivo, Claro, Tim, Oi e Sky são as com maior participação no mercado. A Vivo tem 33% dos clientes de telefonia móvel, 15,5% de banda larga fixa, 26% da telefonia fixa e 28% da TV por assinatura. A Claro tem *market share* de 27,8% (móvel), 23,9% (banda larga), 30,7% (fixa) e 42,9% (TV por assinatura). Em 2022, a Oi era a terceira operadora mais forte, com percentuais de 16,3%, 12,6%, 30,1% e 19,8%, respectivamente. A TIM só tem relevância na telefonia móvel, com 20,3% dos clientes. A Sky só é forte no mercado de TV por assinatura, com 28%. Importante destacar que o setor de banda larga fixa é o que tem mais competição, sendo 48% de outras empresas de menor porte fazendo a distribuição de sinal (BRASIL, 2022a).

Todas as principais empresas do setor são controladas por grupos estrangeiros. A Claro é parte do grupo mexicano América Móvel. A Vivo é controlada pela espanhola Telefónica. A TIM é de uma operadora de telecomunicações italiana. A Sky era de propriedade da norte-americana AT&T, mas foi vendida em 2021 para o

4 Endereço web: https://informacoes.anatel.gov.br/paineis/infraestrutura.

Grupo Werthein, da Argentina (KNOTH, 2023). A Oi, que era brasileira, também mudou de dono: foi comprada por um consórcio formado por Claro, Tim e Vivo (SANT'ANA, 2022).

Para observar a telecomunicação via satélite, a Anatel apresenta um painel exclusivo[5] para espectro e órbita. Em janeiro de 2025, havia 45 satélites geoestacionários, controlados por 26 operadores diferentes. São 31 satélites estrangeiros e 16 brasileiros. Há também 9 sistemas não-geoestacionários, controlados por 10 operadoras, todos estrangeiros. A Anatel considera satélites em operação comercial por banda de radiofrequência, por operadora e de acordo com a posição orbital. Satélites brasileiros são considerados os que usam recursos de órbita e espectro radioelétrico notificado pelo Brasil ou a ele distribuídos ou consignados, cuja estação de controle e monitoração esteja em território nacional.

A norte-americana SpaceX lançou o projeto Starlink, em 2019, que consiste em uma constelação de satélites de baixa órbita para oferecer conectividade à Internet. No Brasil, em março de 2025, a empresa contava com 335 mil clientes, o que representava 60% do mercado de Internet via satélite no país. Eram cerca de 4.400 satélites Starlink sobre o território brasileiro, mas há planos para lançar ao menos 7.500 novos satélites. Alexandre Freire, conselheiro da Anatel, reconhece que na agência há preocupações relacionadas à "*soberania digital*" e à *"segurança de dados e riscos cibernéticos"*, uma vez que a Starlink pode operar fora da jurisdição brasileira e a fiscalização é muito difícil (SÉRVIO, 2025).

A opção brasileira pelo modelo de controle privado das telecomunicações tem demonstrado dificuldades para erradicar a exclusão digital. De acordo com o Comitê Gestor da Internet no Brasil, o país está avançando para atingir a universalização do acesso à Internet, mas com baixa qualidade nos serviços (CGI.br, 2024). O estudo *Conectividade Significativa: propostas para medição e o retrato da população no Brasil* (NIC.br, 2024) mostra que apenas 22% dos brasileiros a partir dos 10 anos de idade têm condições satisfatórias de conectividade. Para 57% da população, o serviço é deficitário. Cerca de 16% não têm nenhum tipo de acesso.

O estudo demonstra que as regiões mais pobres, Norte e Nordeste, têm as piores condições de conectividade significativa. Nesses locais, somente cerca de

5 Endereço web: https://informacoes.anatel.gov.br/paineis/espectro-e-orbita

10% da população têm acesso de qualidade. Já no Sudeste, o número sobe para 31%, o que também é muito pouco. A população rural tem 54% de seu acesso à Internet na faixa de escala de pior nota, segundo os critérios do NIC.br. Em cidades com menos de 50 mil habitantes são cerca de 44%. Cidades com mais de 500 mil pessoas têm 24% na pior faixa de conexão.

Por grupo social, os idosos têm 61% na faixa de pior pontuação. Cor ou raça e nível de escolaridade também são fatores que escancaram a desigualdade. Quanto pior é a condição social, pior é a qualidade do acesso. Nas classes sociais D e E há 64% na pior faixa e apenas 1% na melhor.

Em 2021, a penetração de banda larga móvel era de 96 assinantes para cada 100 habitantes. Para banda larga fixa, o número caía para 19 assinantes para cada 100 habitantes (ADVISIA, 2023, p. 26). O uso de banda larga móvel é adequado para navegação na rede, uso de aplicativos para celulares, troca de mensagens instantâneas e outros serviços rápidos. No Brasil, nenhuma das grandes operadoras oferece pacote ilimitado de dados para *download* nas redes 4G ou 5G. Isso resulta que realizar ações que demandam mais consumo de banda são mais complicadas de serem executadas por quem tem somente Internet via celular. Para atividades profissionais e/ou corporativas, a banda larga fixa é uma necessidade.

No Plano Estratégico da Anatel 2023/2027, espera-se que a cobertura de rede 5G suba de 34,5% (2022) para 57,6% (2027). Planeja-se que a conexão de *backhaul*[6] de fibra ótica alcance 100% de sedes municipais (prefeituras) em 50% das localidades com mais de 600 habitantes. Em 2022, eram 84% dessas sedes municipais e 14% das localidades (*Ibid.*, p. 92). Antes de 2030, a universalização da conectividade não será uma realidade no Brasil.

O Governo Federal, em agosto de 2024, anunciou que o poder executivo mudaria sua concepção sobre compras públicas em telecomunicações e que daria preferência à empresa estatal Telebras para fortalecê-la. Na ocasião, autoridades declararam sobre a importância de se ter uma empresa que seja capaz de levar conectividade aos rincões do país, onde o mercado não chega (AGÊNCIA GOV, 2024). Desde o final de 2023, já havia entrado em vigor a Lei nº 14.744/2023, que favorece a contratação da Telebras e dos Correios pelo poder público.

---

6 NOTA: O *backhaul* é responsável pela ligação entre o *backbone (núcleo da rede) e* as sub-redes periféricas.

3.2.3. *Hardwares* e equipamentos

Segundo dados da Confederação Nacional da Indústria, em 2022, a fabricação de *“equipamentos de informática, produtos eletrônicos e ópticos”* no Brasil empregava cerca de 126 mil pessoas, em quase 3 mil indústrias. Quase toda a produção, aproximadamente 94%, era destinada ao mercado interno. Dentre os itens produzidos estão relógios, celulares, computadores, impressoras, máquinas fotográficas e filmadoras. A participação desse setor no PIB industrial brasileiro era de apenas 1% (CNI, 2022). Apesar de uma planta industrial razoável, os itens fabricados não são de tecnologia de ponta, sendo, em grande parte, apenas montagem de componentes importados.

Em fevereiro de 2025, o Governo Federal publicou uma versão atualizada do *Plano de Ação da Nova Indústria Brasil* (NIB), que pretende alavancar a produção industrial brasileira de maneira geral. O plano foi dividido em missões, sendo que a missão 4 é *“transformação digital da indústria para ampliar a produtividade”* e a missão 6 é *“tecnologias de interesse para a soberania e defesa nacionais”*. A missão 4 abrange semicondutores, robôs industriais, produtos e serviços digitais avançados (plataformas digitais, computação em nuvem e audiovisual). Já a missão 6 tem foco na produção de veículos lançadores, radares e satélites (BRASIL, 2025b).

Dentre os desafios que a NIB pretende superar na missão 4, destacam-se *“formar e capacitar mão de obra em TICs e semicondutores no ensino básico e superior”* e *“minimizar a dependência de soluções importadas, geradas pelo baixo desenvolvimento de hardware no país”*. O plano traça como meta *“transformar digitalmente 25% das empresas industriais brasileiras em 2026 e 50% em 2033, assegurando a participação da produção nacional nos segmentos de novas tecnologias”* (*Ibid.*, p. 69).

Também são pontos da missão 4 *“I. fortalecer e desenvolver empresas nacionais competitivas em tecnologias digitais disruptivas e emergentes, em segmentos estratégicos para a soberania digital e tecnológica”* e *“III. reduzir a dependência produtiva e tecnológica do país em produtos nano e microeletrônicos e em semicondutores, fortalecendo a cadeia industrial das tecnologias da informação e comunicação”* (*ibid.* p. 70).

Os instrumentos que o Governo pretende usar para a NIB são financiamentos reembolsáveis e não reembolsáveis para semicondutores, IA generativa, robótica avançada e tecnologia 6G, além de trabalhar para melhorar a regulamentação, sobretudo para os setores de conectividade e propriedade intelectual. Promete usar o poder de compra pública para ajudar a implementar a *Estratégia Nacional de Governo Digital* e a adoção de Inteligência Artificial no poder público.

Na NIB também está o esforço para reverter o processo de liquidação e promover a retomada operacional do Centro Nacional de Tecnologia Eletrônica Avançada S.A. (Ceitec). A empresa atua em projetos e fabricação de circuitos integrados, *chips*, módulos e *tags* de identificação por radiofrequência. Foi criada como empresa pública para ser um centro estratégico de microeletrônica, em 2008. Durante o Governo Bolsonaro (2019-2022), a orientação era o fechamento da estatal, o que não ocorreu (CNN BRASIL, 2020). Enquanto o mundo sofria com a escassez de *chips*, a antiga gestão queria acabar com a fábrica brasileira. Agora, sob Lula, a Ceitec tenta se reestruturar para voltar a atuar nos mercados nacional e internacional, contribuindo com a formação de mão de obra no setor de semicondutores (BRASIL, 2023a).

A produção de *chips* é central no atual conflito comercial entre Estados Unidos e República Popular da China, que envolve capacidade industrial de fabricação em larga escala, desenvolvimento de novas tecnologias, acesso a reservas minerais e dominação dos mercados globais. Os semicondutores são vitais para o funcionamento de todo tipo de eletrônicos, como as máquinas dos *data centers*, que são ferramentas essenciais para o processamento da computação em nuvem e da Inteligência Artificial.

Villaverde (2023, p. 19) mostra como o Brasil e o mundo padeceram durante a pandemia de COVID-19, quando faltaram *chips* para *smartphones*, automóveis, aviões e sistemas de segurança. As linhas de produção e de montagem de vários setores industriais chegaram a interromper suas produções por falta de componentes eletroeletrônicos. Não é possível falar em *soberania digital* e depender integralmente da importação de *chips* ou de qualquer tipo de produto que contenha semicondutores.

Mesmo a Ceitec voltando a funcionar, sua capacidade de produção está bastante comprometida e demorará algum tempo para que retome níveis anteriores de fabricação. Além disso, a tecnologia brasileira é muito inferior à que encontramos em outros locais, como EUA, Taiwan, Coreia, Singapura, Japão, União Europeia e China. Para Villaverde, o *"Brasil não pode se afastar deste seleto grupo mundial de países que detêm o domínio tecnológico, a capacidade fabril e a expertise no desenvolvimento, a produção e a comercialização de semicondutores"* (ibid., p. 22).

Contudo, como dito anteriormente, a produção de equipamentos de informática, produtos eletrônicos e ópticos é de apenas 1% do PIB industrial (CNI, 2022). Essa categoria integra o setor da indústria de transformação, que, no total, corresponde a 55,4% do PIB industrial (os outros setores são indústria extrativa e indústria da construção). Em 2024, a indústria respondeu por 24,7% do PIB brasileiro (CNI, 2025). As intenções da Nova Indústria Brasil podem ser fantásticas, mas há um longo caminho a percorrer até que o país se torne novamente relevante na produção de *hardware*.

3.2.4. *Data Centers*

A Agência Brasileira de Desenvolvimento Industrial (ABDI) publicou, em 2023, um amplo estudo sobre o mercado de *data centers* no Brasil, em parceria com o Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC). Denominado *Estratégia para a implementação de política pública para atração de data centers*, o documento tem por objetivo identificar como ajudar a aumentar a quantidade de investimentos no setor. Por definição, o estudo considera *data centers* as estruturas físicas e de prestação de serviços especializados de armazenamento, gerenciamento e segurança de dados.

O estudo da ABDI (BRASIL, 2023b, p. 44) traz uma tabela consolidada de quais são os principais fornecedores de *data centers* no Brasil e como se distribuem pelas regiões metropolitanas do país. As empresas listadas eram responsáveis por 61,5% do mercado (*market share*) no período pesquisado.

Tabela 1 – Número de data centers em atividade no Brasil – 2021

Empresas	Número de Data Centers em Operação (junho de 2021)	Áreas Metropolitanas Atendidas
IBM	1	Campinas
Equinix	6	São Paulo e Rio de Janeiro
Ascenty	17	São Paulo, Campinas, Rio de Janeiro e Fortaleza
Tivit	4	Rio de Janeiro, São Paulo e Fortaleza
Scala	2	São Paulo
Lumen	3	Rio de Janeiro, São Paulo e Curitiba
Odata	2	São Paulo e Campinas
HostDime	2	São Paulo e Campina Grande
DXC	2	São Paulo
Embratel	5	Rio de Janeiro, São Paulo e Brasília
Sonda	2	Belo Horizonte e São Paulo
Elea Digital	7	Rio de Janeiro, São Paulo, Brasília, Curitiba e Porto Alegre
Nabiax	2	São Paulo

Nota 1: A IBM é proprietária e opera 1 data center, mas também possui outros data centers alugados de provedores de colocation no Brasil
Nota 2: Para a Odata, estão sendo considerados os data centers SP01 e SP02 divulgados, porém a empresa também administra o data center da T-Systems
Fontes: Relatórios Financeiros e Website de Empresas, pesquisas primárias com empresas e análises da Frost & Sullivan

Fonte: Frost & Sulivan. In: BRASIL, 2023b

Há uma forte concentração de centros de dados nos estados das regiões Sul e Sudeste. São Paulo aparece 13 vezes, Campinas (também no estado de São Paulo) é mencionada três vezes. No Nordeste, Fortaleza-CE aparece duas vezes e Campina Grande-PB é citada uma vez.

As empresas que controlam os data centers listados na tabela são, em maior parte, estrangeiras. São norte-americanas a IBM, a Lumen, a HostDime e a DXC. A Nabiax era espanhola, mas depois vendeu suas operações para a britânica Actis. A Sonda é chilena. A Embratel faz parte do grupo América Móvil (México). São brasileiras a Tivit, a Odata e a Elea Digital. A Scala é brasileira, mas tem parceria com a DigitalBridge (EUA). A Ascenty também é brasileira, com parceria com a Brookfield Infrastructure (Canadá).

O mercado de *data centers* pode ser dividido em três partes. Primeiro, na prestação de serviços de infraestrutura, hospedagem, armazenamento e processamento de dados para clientes de grande porte. Em segundo lugar, há fornecedores de menor capacidade, que prestam serviços para clientes de todos os tamanhos, mas com foco nos de menor necessidade. Em terceiro, há as grandes

empresas de hiperescala, que mantêm operações de *data center* para suprir suas próprias necessidades.

Um exemplo de *data center* de grande porte que não vende serviços para terceiros é o Complexo Capital Digital, em Brasília-DF, construído e operado pelos bancos públicos Banco do Brasil e Caixa Econômica Federal. O *data center* está localizado em um terreno de 40.000 m² e possui 12.770 m² de piso elevado (GCE S/A, [s.d.]). No entanto, apesar de seu tamanho, este *data center* atende apenas aos bancos públicos.

Quanto aos *data centers* de hiperescala mantidos pelas *Big Techs* em solo brasileiro, em 2021, eram 15 locais, todos no estado de São Paulo. Da lista, Amazon, Google, IBM, Microsoft e Oracle são norte-americanas; Alibaba e Tencent são chinesas[7] (BRASIL, *sup. cit.*, 2023b, p. 309).

Tabela 2 – data centers de Cloud Providers, 2021

Provedor de Nuvem	Área metropolitana	Região de nuvem	Quantidade de zonas de disponibilidade
Amazon Web Services (AWS)	São Paulo	São Paulo	3
Google Cloud Platform (GCP)	São Paulo	São Paulo	3
IBM Cloud	São Paulo	São Paulo	3
Microsoft Azure	São Paulo	Brasil Sul	3
Oracle Cloud	São Paulo	Brasil Leste	1
Oracle Cloud	Vinhedo	Brasil Sudeste	1
Alibaba Cloud	-	-	-
Tencent Cloud	São Paulo	São Paulo	1

FONTE: Frost & Sullivan, com base no Cloud Infrastructure Map e nos sites dos provedores de nuvem, até julho de 2022.

Fonte: Frost & Sulivan. In: (ABDI, 2023b)

A pesquisa da ABDI apresenta dados de 2021. Depois disso, muitas empresas anunciaram investimentos na América Latina, principalmente no Brasil, que emergiu como líder na abertura de novos *data centers*, seguido por México, Chile e Colômbia. Em 2023, a Ascenty iniciou as operações de seu 4º centro de dados, em Osasco-SP. A Equinix divulgou investimentos de US$ 132 milhões no

7 NOTA: o estudo não traz informação sobre a localização da Alibaba Cloud.

estado de São Paulo. A Elea Digital lançou um novo *data center* em Porto Alegre-RS, enquanto a V.tal inaugurou um em Fortaleza-CE (RODRIGUES, 2023).

No final de 2024, o jornal *Valor Econômico* publicou uma matéria afirmando que o Brasil vive um *boom* de novos data centers. Segundo a matéria, a receita deste setor no país pode chegar a US$ 1,9 bilhão em 2027. Em 2023, a estimativa era de US$ 1,3 bilhão. O maior impulsionador para o crescimento seria a demanda por adoção de Inteligência Artificial (MARTÍNEZ-VARGAS, 2024).

Os investimentos, custos e despesas para operacionalizar *data centers* envolvem energia, refrigeração, espaço físico, conectividade e telecomunicações, equipamentos de TI, como servidores e *softwares*, mão de obra especializada e pessoal de apoio (vigilância e serviços de limpeza), além de carga tributária (ABDI, sup. cit., 2023, p. 18).

Comparado a outros países, o Brasil apresenta uma melhor vantagem competitiva na geração de energia, principalmente nas renováveis. Por outro lado, segundo entrevistas da ABDI com empresários, a nação peca pela alta tributação, falta de mão de obra, custos trabalhistas e burocráticos (ibid., p.261). Estranho seria se os agentes de mercado não reclamassem dos impostos e dos direitos para os trabalhadores. Essas queixas são padrão, seja qual for o segmento de negócios. Segurança pública e custos com imóveis são outros pontos de atenção.

Para definir a posição competitiva energética, a ABDI usa o índice *Trilemma Energy Index*, publicado pelo World Energy Council (WEC), que avalia três categorias: segurança, equidade e sustentabilidade (*ibid*., p. 263). Dentre 101 países pesquisados, o Brasil fica na 6ª posição em ‘segurança’ e em ‘sustentabilidade’, devido à alta diversificação, potencial energético e matriz renovável. O que derruba a nota brasileira é a categoria ‘equidade’, que considera a cobertura da rede elétrica para a população e os preços de energia, gasolina e diesel. Assim, o Brasil está na 26ª posição geral.

Atrair *data centers* para o Brasil também apresenta riscos. Primeiro, o impacto ambiental causado pelo alto consumo de energia. Multinacionais se instalam para aproveitar o nosso potencial energético, e o lucro obtido com capital intelectual e com a economia de dados é enviado para o exterior. Em segundo lugar, há o risco que esse tipo de atividade passe a rivalizar com o fornecimento de energia e de

água para outras atividades produtivas e também para os cidadãos em geral. Em março de 2025, o jornal britânico The Guardian publicou o artigo questionando se o aumento do número de *data centers* no Brasil não poderia deixar as pessoas comuns no escuro (LIMA, 2025). Mesmo a matriz energética brasileira sendo limpa, em momentos em que os reservatórios estiverem baixos, as termoelétricas deverão ser acionadas, produzindo mais poluição e tornando os preços mais caros para a sociedade, pressionando a inflação.

Para prevenir-se de problemas futuros, a Microsoft, em busca de previsibilidade para manutenção de seu modelo de negócios, assina contratos especiais de compra e venda de energia, Um exemplo é o acordo com a AES Brasil para aquisição de energia eólica renovável por 15 anos. A energia será gerada pelo Complexo Eólico Cajuína, no Rio Grande do Norte. Comparativamente, a eletricidade produzida seria suficiente para o consumo de 250 mil residências (MICROSOFT, 2023).

3.2.5. *Softwares* básicos

As camadas de infraestrutura apresentadas até aqui foram as físicas (produção de energia elétrica, telecomunicações, fabricação de *hardwares* e instalação de *data centers).* As próximas quatro são as camadas lógicas, que têm por característica ser intangíveis. S*oftwares*, dados e algoritmos são tão ou mais importantes do que infraestruturas físicas.

Os equipamentos de informática precisam de um sistema básico para poder funcionar, que também pode ser chamado de sistema operacional. Há quatro tipos principais de sistemas operacionais: 1. para computadores de mesa (*desktops* e *notebooks*); 2. para dispositivos móveis (*smartphones* e *tablets*); 3. sistemas embarcados (para diversos tipos de equipamentos específicos); e 4. para servidores (que são as máquinas que rodam dentro dos *data centers*).

O *site* statcounter.com permite verificar quais são os sistemas operacionais mais utilizados no mundo. O portal rastreia mais de 1,5 milhão de endereços *web*, o que possibilita conhecer o *market share* dos sistemas por plataforma. Em fevereiro de 2025, o *site*, no agregado geral, mostrava como sistema mais usado o

Android/Google (desenvolvido com um kernel Linux), com 45,5% de participação. Em segundo lugar está o Microsoft Windows, com 25,36%, seguido pelos sistemas da Apple, o iOS (iPhone), com 18,2%, e o OSX (macOS), com 5,65%.

Se forem considerados apenas *desktops* e *notebooks*, o Windows tem 70,54% do mercado global e a Apple tem 15,77%. Para dispositivos móveis, o Android tem 71,75%, enquanto o iPhone conta com 27,78%.

Os sistemas operacionais para servidores, que são a base de funcionamento da computação em nuvem, têm o Linux como dominante, com 63,1% de presença nos servidores dos Estados Unidos (FORTUNE BUSINESS INSIGHTS, 2025). O Linux tem como características o licenciamento como *software livre*, o código-fonte aberto, ser de baixo custo, ter alta performance, compatibilidade e segurança.

Softwares livres são sistemas licenciados pela GNU/General Public License (GNU/GPL) ou por outra licença similar. A GNU/GPL permite a qualquer pessoa usar o sistema, estudá-lo, adaptá-lo e redistribuí-lo. A única restrição é que, caso o usuário faça alterações, ele não poderá fechar o código alterado. Precisará redistribuir as modificações à comunidade internacional de desenvolvedores daquele programa. O acesso ao código-fonte permite que qualquer estudante tenha as mesmas oportunidades de aprender e de se aperfeiçoar que qualquer engenheiro que trabalha em uma empresa multinacional.

Não exigir pagamento de licenças proprietárias permite que os *data centers* cresçam sua capacidade operacional sem preocupações com custos de licenciamento de *software*. Porém, os números de crescimento do sistema Windows também vêm aumentando, devido à necessidade de os provedores de nuvem oferecerem ambientes híbridos aos seus clientes (*Ibid*.).

O licenciamento como *software* livre elimina uma das barreiras de entrada do mundo virtual, que é a propriedade intelectual restritiva nos sistemas computacionais. O Brasil iniciou uma política tecnológica para melhorar a sua autonomia nesta camada, mas a abandonou progressivamente, acabando oficialmente com ela em 2016, pouco antes de ocorrer o golpe que derrubou a Presidenta Dilma Rousseff.

Entre os anos de 2003 e 2016, o Governo Federal manteve o Comitê de Implementação de *Software* Livre (CISL), que estimulava a adoção de sistemas

abertos pela administração pública e pela sociedade em geral, conforme relatei em minha dissertação de mestrado (CASSINO, 2019). Defendia-se um amplo programa de capacitação da juventude com tecnologias abertas para suprir as demandas por mão de obra especializada em tecnologias da informação no país.

Um programa de formação em TICs em larga escala não precisa ser necessariamente com *software* livre. Porém, como política pública, não usar recursos do estado para favorecer treinamentos em produtos de empresas privadas estrangeiras é desejável. O fato de a adoção de programas de computador com licenças livres (e gratuitas) dispensar licitação também permite celeridade para implementar os cursos. Um exemplo são as inúmeras iniciativas de inclusão digital e capacitação com Linux e outros sistemas livres, como os Telecentros da Prefeitura Municipal de São Paulo, criados em 2001.

A demanda por profissionais de TICs no mercado brasileiro está bastante aquecida. Estima-se um *deficit* de 530 mil profissionais até o final de 2025 (JOSÉ, 2024). A procura é muito superior à capacidade de formar novos profissionais habilitados a trabalhar no setor. As áreas com mais carência são Inteligência Artificial, segurança da informação, e criação de infraestrutura e desenvolvimento de sistemas. São áreas em que os *softwares* livres são particularmente poderosos, o que permitiria que cursos patrocinados pelo poder público para aumento da inteligência coletiva suprissem também as necessidades das empresas.

Softwares livres são usados em sistemas de missão crítica, e há multinacionais especializadas em vender subscrições e serviços de suporte de suas próprias versões de Linux[8]. São exemplos as norte-americanas Red Hat Enterprise Linux e Oracle Linux, a sul-africana Canonical Ltd. (responsável pelo Ubuntu Linux) e a alemã SUSE Linux. Esta última é parceira estratégica da Microsoft para o uso de Linux na nuvem Azure.

A Microsoft, inclusive, passou por uma mudança radical de postura em relação ao Linux. No início dos anos 2000, considerava o sistema livre como inimigo, como uma ameaça ao seu modelo de negócios de venda de licenças proprietárias. Cerca de 15 anos depois, na metade da década de 2010, a empresa lançou a campanha *“Microsoft Loves Linux”* e passou a contribuir ativamente com o

8 NOTA: Linux e software livre não são sinônimos. Linux é o principal sistema operacional livre. Softwares livres são quaisquer programas de computador licenciados pela GNU/GPL ou similar.

desenvolvimento de soluções de código aberto. A transformação ocorreu porque o modelo de negócios da Microsoft mudou. Hoje é muito mais baseado em serviços de nuvem do que na venda de licenças (MICROSOFT, 2015).

3.2.6. Desenvolvimento de sistemas

De acordo com o relatório *Mercado Brasileiro de Software 2024 – Panoramas e Tendências*, da Associação Brasileira das Empresas de Software (ABES), o Brasil é o 10º maior mercado de Tecnologia da Informação do mundo (em 2023), movimentando US$ 49,9 bilhões. No contexto global, a soma de todos os países é de US$ 3,1 trilhões. Os EUA, sozinhos, respondem por US$ 1,2 trilhão. O mercado chinês, que vem na 2ª posição, com US$ 361 bilhões, é sete vezes maior que o brasileiro. Na América Latina, o Brasil é soberano, com 37,5% (ABES, 2024).

Dos US$ 49,9 bilhões do mercado brasileiro, a categoria '*software*' equivale a US$ 15 bilhões (30,1% do total). As outras categorias são 'serviços' (22,1%) e '*hardware*' (47,8%). Do montante de valor da categoria '*software*', US$ 3,7 bilhões (24,8%) são decorrentes de sistemas desenvolvidos no Brasil. Deles, apenas US$ 225 milhões (1,5%) foram *softwares* brasileiros vendidos como exportação. Os sistemas estrangeiros vendidos no Brasil somaram US$ 11,2 bilhões (73,7%).

Portanto, o *software* brasileiro é minoritário dentro do Brasil e a exportação é pouco significativa. Segundo a ABES, quanto ao tipo de negócio, em 2023, 24,1% (9.062 empresas) atuavam com 'desenvolvimento e produção', 36,4% (13.684 empresas) com 'distribuição e comercialização' e 39,5% (14.856 empresas) com 'prestação de serviços'. Cerca de 92,4% dessas empresas tinham menos de 100 funcionários, sendo consideradas micro ou pequenas (*Ibid.*).

É importante considerar que o capital intelectual, a inovação e o trabalho criativo estão principalmente concentrados na categoria 'desenvolvimento e produção', que é a menor das subcategorias de *software* do mercado brasileiro. Revendas e serviços empregam pessoas e movimentam a economia, mas pouco agregam em inventividade de novas soluções.

Quanto ao consumo de aplicações pelo público brasileiro, o licenciamento em nuvem de aplicações colaborativas (e-mail, conferências, redes sociais,

sincronização de arquivos e *software* compartilhado) correspondia a 91%. O licenciamento tradicional tinha apenas 9% (*Ibid*.).

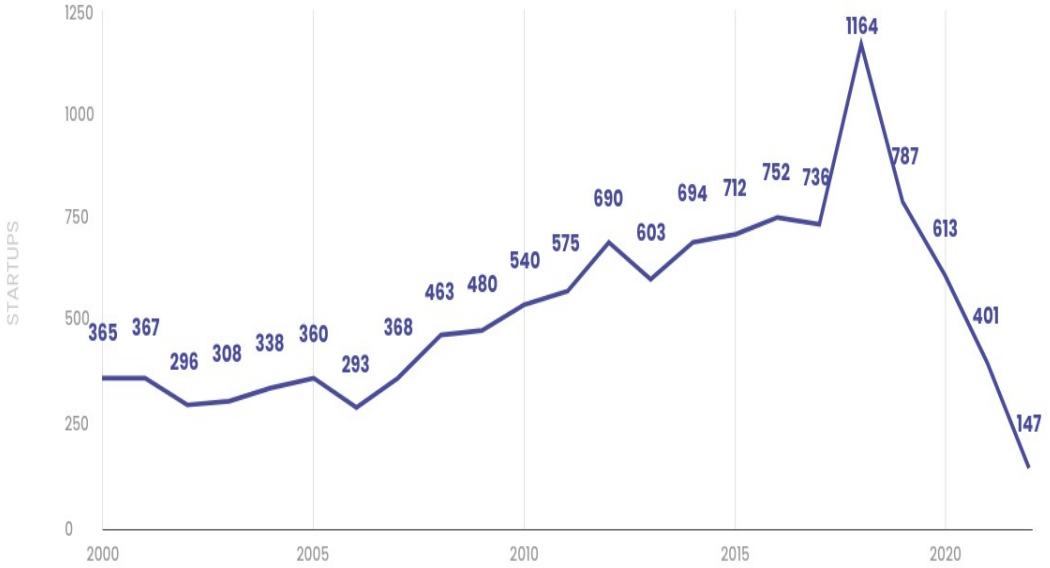
O Brasil conta com 217 milhões de celulares ativos, o que equivale numericamente a 102% de sua população. Cerca de 86% das pessoas usam a Internet. A audiência do público brasileiro é essencialmente baseada em serviços de nuvem (KEMP, 2025). De acordo com dados do *site* datareportal.com, em janeiro de 2025, eram 144 milhões de usuários de redes sociais. Dentre as oito mais acessadas, sete eram norte-americanas e apenas uma era chinesa (TikTok).

Redes sociais mais acessadas no Brasil, em Janeiro de 2025:

- YouTube – 144 milhões;
- Instagram – 141 milhões;
- Facebook – 112 milhões;
- TikTok – 91,7 milhões;
- LinkedIn – 81 milhões;
- Pinterest – 40,3 milhões;
- X/Twitter – 16 milhões;
- Snapchat – 6,7 milhões.

Adeptos da teoria neoliberal costumam defender a criação de *startups* como a resposta milagrosa para melhorar a situação do desenvolvimento de *software* e da criação de soluções inovadoras. A realidade, porém, demonstra a dificuldade de se abrir e manter uma empresa no país. Em 2023, havia 12.040 *startups* ativas, mas o número de abertura de novas empresas cai a cada ano. O pico foi de 1.164 empresas abertas em 2018, mas desabou para apenas 147 aberturas em 2022, uma queda de 87% (SOFTEX, 2024). É verdade que nesse período ocorreu a pandemia de COVID-19, que atrapalhou bastante a economia.

Figura 9 – Startups abertas no Brasil entre 2000 e 2022

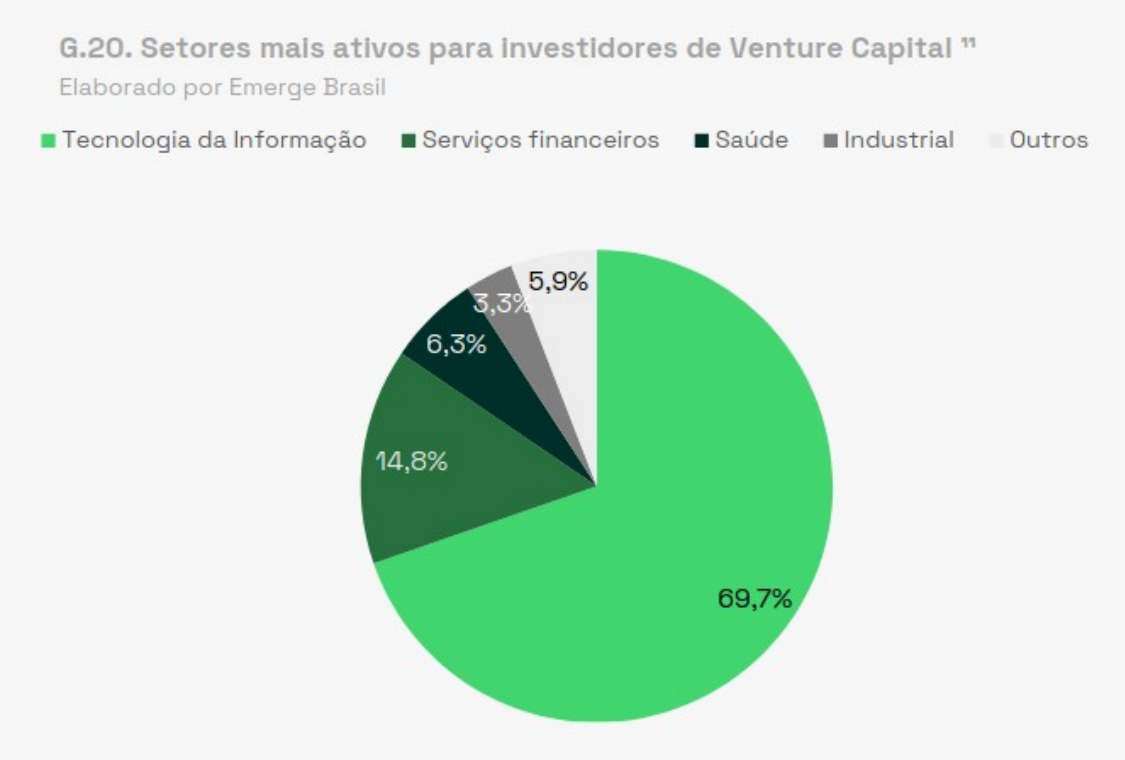


Fonte: Observatório Softex, a partir de dados da Cortex, 2023.

Dados mais recentes, levantados pelo Instituto Brasileiro de Geografia (IBGE), publicados em dezembro de 2024, mostram que 20% das empresas fecham as portas no 1º ano de atividade. Há uma alta taxa de mortalidade empresarial, com apenas 37,3% sobrevivendo após 5 anos. Na categoria ‘informação e comunicação’ do IBGE, a taxa de sobrevivência é um pouco melhor, com 43,8% (PODER36O, 2024b).

Havia quase 900 *startups* de base tecnológica no Brasil, segundo o *Relatório Deep Techs Brasil 2024*, elaborado pela consultoria Emerge. Cerca de 70% dessas empresas estão na região Sudeste. O estado de São Paulo concentra 55% do total. O relatório mostra que há forte dependência do setor público para financiamento, como por meio de editais de fomento ou de subvenção econômica. No caso das que receberam mais de R$ 5 milhões de investimento, 70% utilizaram recursos públicos. Apenas 30% das *startups* passaram às fases de escalonamento, comercialização e expansão, sendo que a demora para isso costuma ser maior do que cinco anos, segundo o relatório. Para quem é do setor de Tecnologia da Informação, a boa notícia é que essa área recebe quase 70% dos investimentos de capital de risco (ALISSON, 2024; EMERGE, 2024).

Figura 10 – Setores mais ativos para investidores de Venture Capital



Fonte: Emerge, 2024

Por fim, um ponto que merece atenção é como as *startups* brasileiras de desenvolvimento de sistemas escolhem seus *frameworks*. Resumidamente, *frameworks* são estruturas que facilitam o desenvolvimento de *software*, sendo compostas por bibliotecas e ferramentas pré-definidas, que poupam muito trabalho dos programadores, que podem focar na construção do seu aplicativo e evitar atividades repetitivas. Os tipos de *frameworks* variam conforme o objetivo: podem ser para desenvolvimento *web* ou voltados para aplicativos móveis, por exemplo.

Há *frameworks* que se baseiam na filosofia do *software* livre e do *open source*, mas também há *frameworks* proprietários, mantidos por empresas privadas. Os de modelo livre garantem mais liberdade de participação, contribuição e colaboração, tendo uma comunidade de participantes como força motriz. Já os proprietários podem oferecer algumas vantagens, como assistência técnica profissional e suporte contratado.

A decisão correta ao selecionar um *framework* é crucial. A *startup* pode ficar presa a um tipo de modelo de desenvolvimento. Migrar para uma alternativa

posteriormente pode ser bem complicado e caro. Ao optar por *frameworks* proprietários, a *startup* praticamente se vincula a um fornecedor. Fica sujeita a mudanças de preços e a alterações de políticas tecnológicas ou contratuais. Por outro lado, a empresa se beneficia de pacotes bem elaborados pelas *Big Techs* para fidelizar quem aderir aos seus produtos e serviços.

A iniciativa *Google for Startups* (startup.google.com), por exemplo, oferece uma variedade de programas, suporte especializado e orientação, que, segundo a multinacional, serve para ajudar as novas empresas a crescer e a ganhar escala. A Microsoft também tem uma iniciativa similar, que oferece um pacote especial para quem está começando. Segundo o *site* da corporação, pode-se receber até US$ 150.000,00 em créditos do Azure ou outros produtos (https://www.microsoft.com/pt-br/startups).

Para um país que deseja aumentar sua soberania tecnológica com desenvolvimento de sistemas, investindo recursos com editais de fomento e com subvenção, o modelo baseado em *startups* apresenta algumas limitações. Primeiro, é que se a seleção de *framework* for feita com base em estruturas estrangeiras, o pedaço de código desenvolvido no Brasil dependerá de um ecossistema que está fora do controle do pequeno empresário nacional. Em segundo lugar, se a *startup* der certo e começar a fazer muito sucesso e dinheiro, ela pode ser comprada por uma *Big Tech*. Se já utilizavam *frameworks* e metodologias proprietárias de quem adquiriu, a integração torna-se extremamente fácil para aquele comprador.

3.2.7. Bases de dados

No capítulo 1 desta tese, foram apresentados diversos autores que mostraram como os dados são os insumos mais importantes nesta fase de *capitalismo digital-dataficado*. O mecanismo consiste em realizar a coleta de dados em larga escala para que seja possível conhecer os consumidores e oferecer-lhes produtos de maneira personalizada. Os dados também são a base para alimentar a Inteligência Artificial, que precisa de quantidades gigantescas de informações para alimentar seus grandes modelos de linguagem (LLMs – *Large Language Models*).

O Estado brasileiro, responsável por uma população de cerca de 211 milhões de habitantes (2023), a sexta maior do planeta, produz e guarda bases de dados riquíssimas, que são de grande interesse das corporações de tecnologia. São exemplos dessas bases o CadÚnico – Cadastro Único para Programas Sociais do Governo Federal; os dados de saúde da população produzidos pelo DATASUS – Departamento de Informática do Sistema Único de Saúde; os dados da Previdência Social, processados pela Dataprev – Empresa de Tecnologia e Informações da Previdência; e as informações de educação geridas pelo Inep – Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. Caberiam ainda bases de dados relativas à Receita Federal, assuntos militares, diplomacia e de inteligência, da administração pública e do funcionalismo público, dentre muitas outras.

Defender essas e outras bases de dados deveria ser assunto prioritário quando se trata de soberania e segurança nacional. O Governo Federal mantém oficialmente o Catálogo de Bases de Dados (CBD), que se propõe a centralizar informações de bases de dados custodiadas pela administração pública federal, conforme orientações do Decreto nº 8.777, de 11 de maio de 2016, e do Decreto nº 10.046, de 9 de outubro de 2019. De acordo com o portal do Governo Digital (BRASIL, 2019b), o CBD, em sua versão 1.1, atualizada em novembro de 2024, conta com 304 bases de dados cadastradas, sendo que 108 delas são de informações sigilosas. Dentre os objetivos declarados do CBD está a necessidade de proteger dados e fomentar a aderência à Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018).

Sem dúvidas, a aprovação da LGPD melhorou o ambiente regulatório quanto à proteção da privacidade *online*, estabelecendo práticas de transparência, regras de tratamento e de coleta de dados, inspirada no modelo europeu (Regulamento Geral de Proteção de Dados – GPDR). Mas ainda é preciso avançar muito para que tenhamos mais segurança na proteção do apetite das empresas de tecnologia por dados, assim como para aperfeiçoar os sistemas de fiscalização.

As empresas devem, pela LGPD, permitir aos titulares dos dados que façam suas próprias escolhas sobre como suas informações são utilizadas. Na prática, o que acontece, na maior parte das vezes, é que os serviços digitais implementaram alertas aos usuários no momento do primeiro acesso. O usuário deve concordar com

as políticas do fornecedor ou abandonar o sistema. São raras as pessoas que param para ler os termos de uso dos produtos antes de começar a usá-los. Não existe opção real. Em muitos casos, como em situações de exigência profissional ou educacional, a pessoa concorda com os termos ou tem que desistir do emprego ou de um curso.

Um dos maiores problemas para a proteção de dados é a capacidade de aplicação extraterritorial das leis brasileiras. Pela LGPD, suas regras valem para o tratamento de dados de indivíduos localizados no território nacional ou para dados que tenham sido coletados no território nacional. Como o Estado brasileiro não tem capacidade de obrigar empresas localizadas fora de sua jurisdição a cumprir a lei nacional, assina acordos bilaterais de cooperação. Com os Estados Unidos, sede das principais empresas de tecnologia, o Brasil mantém um acordo judiciário chamado MLAT – *Mutual Legal Assistance Treaty*, desde 2001.

Joyce Ariane de Souza (2023, p. 207) descreve a pressão do setor privado para o estabelecimento de um sistema de *Open Health* (saúde aberta), com o qual empresas poderiam compartilhar entre si dados de saúde dos usuários de serviços médicos, inclusive os do Sistema Único de Saúde (SUS). De interesse comercial de planos de saúde, farmacêuticas e seguradoras, esse tipo de medida pode agravar distorções discriminatórias, como empresas recusando contratos com clientes com base no histórico de saúde ou na possibilidade de vir a desenvolver uma doença.

O *OpenHealth* quer fazer com o setor de saúde o mesmo que o setor financeiro já fez com o *Open Finance*. Segundo a definição do Banco Central do Brasil, o sistema financeiro aberto significa:

> *"O Open Finance, ou sistema financeiro aberto, é a possibilidade de clientes de produtos e serviços financeiros levarem suas informações das suas instituições de relacionamento para outras e movimentarem suas contas bancárias a partir de diferentes plataformas e não apenas pelo aplicativo ou site do banco onde tem sua conta ou outro serviço contratado, de forma segura, ágil e conveniente".*
> *(BANCO CENTRAL DO BRASIL, [s.d.])*

De acordo com a legislação em vigor, o compartilhamento de dados públicos precisa observar a classificação por grau de sigilo, conforme disposto nos artigos 27

e 28 do Decreto nº 7.724, de 16 de maio de 2012, da Presidência da República. Um dado pode ser categorizado como *ultrassecreto*, *secreto* ou *reservado*.

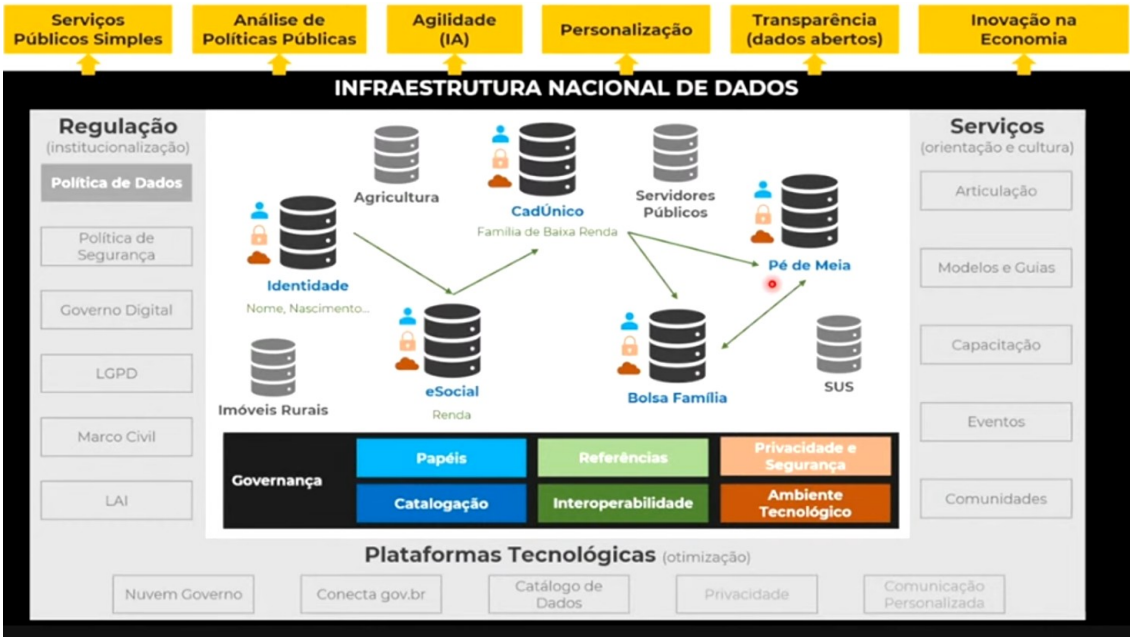
> *"Art. 27. Para a* ***classificação da informação em grau de sigilo,*** *deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:*
>
> *I - a gravidade do risco ou dano à segurança da sociedade e do Estado; e*
> *II - o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.*
>
> *Art. 28. Os prazos máximos de classificação são os seguintes:*
>
> ***I - grau ultrassecreto:*** *vinte e cinco anos;*
> ***II - grau secreto:*** *quinze anos; e*
> ***III - grau reservado:*** *cinco anos.'*
>
> (Decreto Nº 7.724/2021, grifo nosso)

Respeitadas as limitações legais, a *Estratégia Nacional de Governo Digital*, documento do Governo Federal, em seu *Objetivo 7 – Ecossistema de Inovação, Recomendação 7.6*, estimula o uso de dados públicos para promover inovação e exploração econômica:

> ***"Recomendação 7.6.***
> *Utilizar infraestrutura tecnológica que facilite o uso de dados de acesso público e promova a interação entre diversos agentes, de forma segura, eficiente e responsável, para estímulo à inovação, à exploração de atividade econômica e à prestação de serviços à população."*
> *[Estratégia Nacional de Governo Digital]*
> *(BRASIL, 2024c)*

Para implementar o que está previsto na estratégia nacional, legislação e demais documentos oficiais, a Secretaria de Governo Digital (SGD) tem como uma de suas iniciativas estabelecer e manter a Infraestrutura Nacional de Dados (IND). A Figura 11, extraída de apresentação de Renan Gaya Santos, Diretor do Departamento de Infraestrutura de Dados Públicos da SGD, mostra como está dividida a IND.

Figura 11 – Infraestrutura Nacional de Dados, 2024



Fonte: SANTOS, 2024

Para a SGD, a Infraestrutura Nacional de Dados deve ter por objetivo maior suportar diversas aplicações, como serviços públicos, análise de políticas públicas, agilidade [de alimentação] de Inteligência Artificial, personalização, transparência pública (dados abertos) e inovação na economia.

Para tanto, faz-se necessário observar aspectos regulatórios e institucionais, como política de dados, política de segurança, regras do Governo Digital, legislações específicas – como a Lei Geral de Proteção de Dados Pessoais, o Marco Civil da Internet e a Lei de Acesso à Informação – e aspectos de governança (papéis, referências, privacidade e segurança, catalogação, interoperabilidade e ambiente tecnológico).

Somam-se à IND os serviços prestados pela SGD a outros órgãos do governo, tais como articulação, produção de modelos e de guias, capacitação, participação em eventos e estímulo ao funcionamento de comunidades. Quanto às plataformas tecnológicas que compõem o ambiente da IND, destacam-se a Nuvem Governo, o Conecta.gov.br e o Catálogo de Bases de Dados (CBD).

3.2.8. Inteligência Artificial

O último item de nossa lista de infraestruturas do digital é Inteligência Artificial. Talvez ela pudesse estar incluída na mesma categoria que '*software*'. Porém, dado o peso que este assunto tem nos debates atuais sobre Tecnologias da Informação e da Comunicação, a IA merece uma categoria própria.

Além disso, a Inteligência Artificial, como existe hoje, tem características específicas para que possa funcionar, exigindo uma quantidade enorme de dados para enriquecimento de *machine learning* e *deep learning* e uma capacidade assustadora para processamento de suas operações matemáticas.

Inteligência Artificial e a produção de chips e semicondutores são talvez as duas principais tecnologias de futuro, cuja disputa pelo seu domínio é a linha de frente no conflito tecnológico entre Estados Unidos e República Popular da China.

Em 2024, o Governo Federal do Brasil realizou a 5ª Conferência Nacional de Ciência, Tecnologia e Inovação (V CNCTI), na qual o tema da Inteligência Artificial foi central. Na mesa de abertura do evento, o Presidente da República Luiz Inácio Lula da Silva lançou o *Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028*, que estabelece as ações que o país desenvolverá para se integrar nesse campo (CORREIA, 2024).

Além do Plano Brasileiro de Inteligência Artificial, já existia outro documento denominado *Estratégia Brasileira de Inteligência Artificial* (EBIA), mas é datado de 2021 e está em fase de revisão pelo MCTI para que se compatibilize com o PBIA, portanto será desconsiderado nesta tese.

"Soberania tecnológica e de dados" é uma das dez premissas do PBIA (BRASIL, 2024d). De acordo com o plano, o Brasil aportará R$ 23 bilhões entre os anos de 2024 e 2028, estando compatível com os investimentos públicos de outras nações como Alemanha (R$ 29 bilhões em 7 anos), França (R$ 14 bilhões até 2030), Itália (R$ 6 bilhões) e Reino Unido (R$ 18 bilhões).

No entanto, esse segundo grupo de países está bem atrás de EUA e China. Os Estados Unidos tiveram R$ 63 bilhões de investimento público em IA entre 2021-

2024 e mais R$ 380 bilhões de investimentos privados em 2023. Na China foram R$ 306 bilhões em *data centers* em 2024 e R$ 39 bilhões em 2023 (*Ibid.*).

Em janeiro de 2025, o presidente norte-americano Donald Trump anunciou o projeto de IA chamado Stargate, que receberia ao menos US$ 500 bilhões, em parceria com *Big Techs* como Oracle e OpenIA (AFP, 2025). Uma semana depois, veio a resposta chinesa: uma *startup* de Hangzhou lançou a ferramenta de Inteligência Artificial chamada *DeepSeek*, derrubando o valor de mercado de empresas dos Estados Unidos nas bolsas de valores ao redor do mundo (CNN BRASIL, 2025). A solução chinesa seria mais barata, eficiente e acessível do que as rivais ocidentais, segundo relata matéria da CNN.

Voltando ao Plano Brasileiro de Inteligência Artificial, ele define IA como sistemas que "*produzem resultados a partir de um grande volume de dados, permitindo um processo de aprendizagem, que realiza previsões, classificações, recomendações ou gera decisões que possam influenciar ambientes físicos e virtuais"* (BRASIL. *sup. cit.*, 2024d, p. 6).

O PBIA é dividido em três partes: 1. ações de impacto imediato (que são ações de curtíssimo prazo para resolver problemas específicos); 2. ações estruturantes (divididas em eixos); e 3. gestão e monitoramento.

As ações estruturantes são divididas em cinco eixos:

- Eixo 1: Infraestrutura e Desenvolvimento de IA;
- Eixo 2: Difusão, Formação e Capacitação em IA;
- Eixo 3: IA para Melhoria dos Serviços Públicos;
- Eixo 4: IA para Inovação Empresarial;
- Eixo 5: Apoio ao Processo Regulatório e de Governança da IA.

A Tabela 3 mostra como os valores previstos para investimento se distribuem em cada uma das partes. Os valores que serão destinados para inovação empresarial consomem mais de 50% dos recursos que serão destinados ao PBIA.

Tabela 3 – Investimentos previstos para o PBIA 2024-2028

Descrição	2024-28
Ações de Impacto Imediato	R$ 435,04 milhões
Infraestrutura e Desenvolvimento de IA	R$ 5,79 bilhões
Difusão, Formação e Capacitação em IA	R$ 1,15 bilhões
IA para Melhoria dos Serviços Públicos	R$ 1,76 bilhão
IA para Inovação Empresarial	R$ 13,79 bilhão
Apoio ao Processo Regulatório e de Governança da IA	R$ 103,25 milhões
Total	R$ 23,03 bilhões

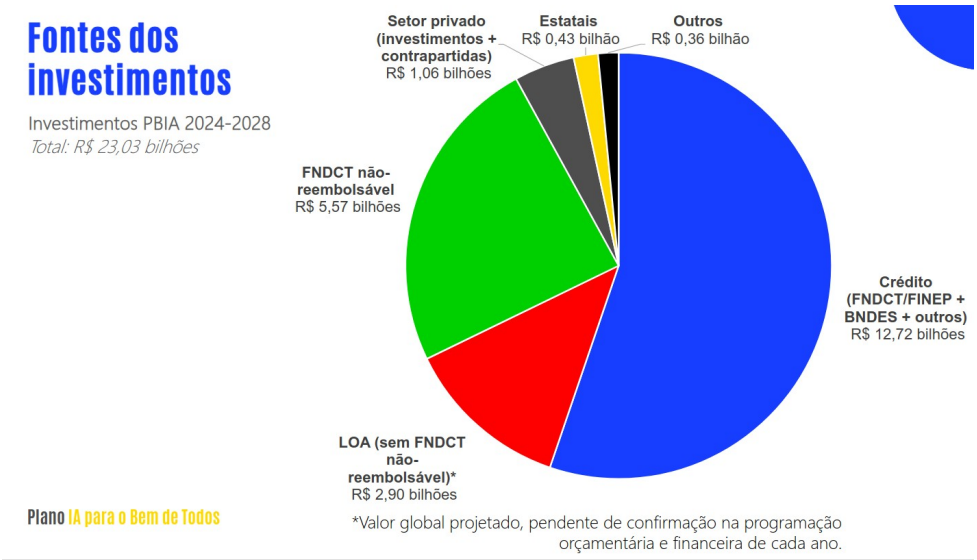
Fonte: PBIA (BRASIL, 2024d)

Das fontes previstas para investimentos no PBIA, do setor privado, que é destinatário de mais da metade dos recursos, o Governo Federal espera R$ 1,06 bilhão, somando investimentos e contrapartidas. Das verbas que vêm do governo, R$ 12,72 bilhões referem-se a crédito (empréstimos que precisam ser devolvidos mediante pagamento de juros, ainda que mais baixos se comparados com as tarifas praticadas pelo mercado bancário). De recursos não-reembolsáveis, estão previstos R$ 8,47 bilhões, sendo que R$ 5,57 bilhões são provenientes do Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT).

Para efeito de comparação, em 2025, o orçamento total do FNDCT aprovado é de R$ 14,7 bilhões (BRASIL, 2025c). O PBIA pretende destinar R$ 5 bilhões do fundo somente para IA, entre 2024 e 2028.

A Figura 12 detalha quais são as demais fontes do PBIA.

Figura 12 – Fontes dos investimentos do PBIA 2024-2028



Fonte: BRASIL, 2024d

Para os objetivos desta tese, o eixo do PBIA que merece mais atenção é o Eixo 1 – Infraestrutura e Desenvolvimento de IA, que pretende *"posicionar o Brasil como um líder mundial em Inteligência Artificial, impulsionando projetos e pesquisas que melhorem substancialmente a vida dos brasileiros, com soluções inovadoras e acessíveis para os desafios do país"* (BRASIL. *sup cit.*, 2024d, p. 43). O Eixo 1 é subdividido em quatro programas:

1. Programa Nacional de Infraestrutura para IA;
2. Programa de Sustentabilidade e Energias Renováveis para IA;
3. Programa de Estruturação do Ecossistema de Dados e *Software* para IA;
4. Programa de Pesquisa e Desenvolvimento em IA.

O PBIA destaca cinco ações do Eixo 1 que devem receber atenção especial:

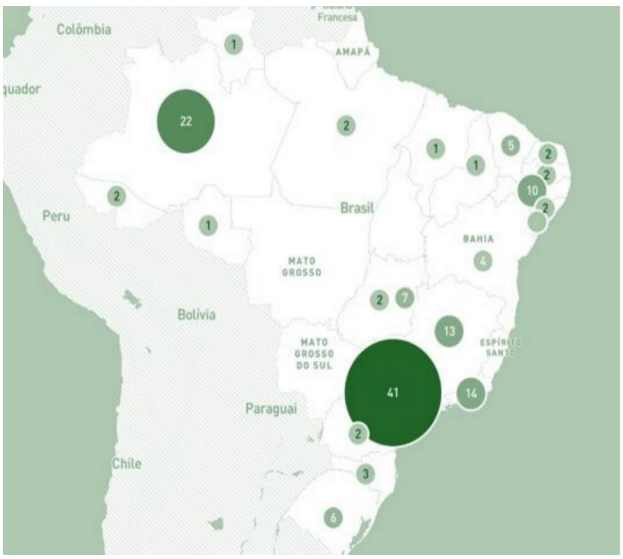
1. Investir em um supercomputador que figure entre os cinco maiores do mundo em capacidade de processamento para impulsionar a pesquisa de ponta no Brasil;

2. O desenvolvimento nacional de processadores de IA de alto desempenho em projetos de cooperação internacional;
3. Infraestrutura de IA sustentável (baseada em energias renováveis);
4. Modelos de linguagem em português de nível mundial, garantindo redução de vieses e soberania de dados para o Brasil;
5. Criar uma Rede nacional de centros de excelência em IA, fomentando a pesquisa em todas as regiões do país.

Um ponto bastante curioso do plano de IA é que o Governo Federal conta como infraestrutura a “nuvem soberana” do Serpro, que está sendo implementada em parceria com *Big Techs* norte-americanas e chinesas. Para montar a “Nuvem de Governo”, a estatal gastará R$ 710 milhões (SERPRO, 2024b). Este assunto será aprofundado no próximo capítulo.

Quanto aos laboratórios de pesquisa em IA no Brasil, a Figura 13 mostra como está a atual distribuição geográfica. Chama a atenção o estado do Amazonas, na Região Norte, como segundo ponto de concentração do país, uma vez que a maior parte dos investimentos no setor acaba sendo tradicionalmente direcionada para a Região Sudeste. Conforme o mapa, São Paulo tem 41 unidades, o Amazonas tem 22, o Rio de Janeiro tem 14, Minas Gerais tem 13 e Pernambuco tem 10.

Figura 13 – Distribuição de laboratórios de IA no Brasil



Fonte: Observatório de Tecnologias Digitais, CGEE

CAPÍTULO 4
A “NUVEM SOBERANA” DO BRASIL

O fortalecimento da *soberania digital* de um país só ocorre se cada uma das infraestruturas do digital for encarada como parte de um ecossistema complexo, sobre o qual o Estado precisa ter capacidade real de intervenção, mesmo que evite tomar atitudes intervencionistas.

Para tanto, o Estado precisa ter uma visão clara sobre a questão e formalizá-la em documentos públicos que sinalizem seu potencial de atuação. Porém, o que temos no Brasil são planos e estratégias, quase sempre superficiais, e que atendem ao gosto do mercado privado. Um desses documentos é a *Estratégia Brasileira para a Transformação Digital (E-Digital) – Ciclo 2022-2026* (BRASIL, 2022b).

Sérgio Amadeu da Silveira (2024, p. 11-25) denunciou a atual onda denominada “transformação digital” como parte da ideologia do Vale do Silício, que apresenta as inovações tecnológicas como neutras, mas traz em si traços centrais da doutrina *neoliberal* e uma combinação da doutrina *positivista*, na qual a tecnologia seria sempre um meio, nunca uma finalidade. Adotar a terminologia neoliberal já é uma forma de trazer para dentro do Estado as práticas que favorecem as corporações multinacionais e enfraquecem a *soberania digital* e a capacidade de intervenção.

As infraestruturas físicas do digital (produção de energia, redes de telecomunicações, *data centers* e fábricas de equipamentos), por estarem baseadas em solo nacional, podem ser obrigadas pelo Estado a cumprir suas leis e determinações judiciais. Em uma situação extrema, as instalações podem ser tomadas por forças militares e até a ser nacionalizadas ou expropriadas.

Com as infraestruturas lógicas é diferente. *Softwares* são ativos intangíveis, que trafegam pelas redes de informação na velocidade da luz, o que torna muito mais difícil o controle soberano sobre eles.

Os dados, relembrando Couldry e Mejías, são o maior insumo do mundo digital. São o que verdadeiramente geram valor para as *Big Techs*. Varoufakis mostrou como a prática de capturar dados produzidos por terceiros e lucrar sobre eles faz as Big Techs serem como rentistas tecnofeudais.

Proteger o Brasil da fuga de dados, especialmente das grandes bases de dados do Estado, é fundamental para a construção da soberania nacional, mas na *Estratégia Brasileira para a Transformação Digital* (E-Digital), talvez o principal documento oficial sobre rumo futuro do país no campo das TICs, a palavra “soberania” não aparece nenhuma vez.

A estratégia brasileira é composta por cinco Eixos Habilitadores: 1. infraestrutura e acesso às Tecnologias de Informação e Comunicação; 2. pesquisa, Desenvolvimento e Inovação (PD&I); 3. confiança no ambiente digital; 4. educação e capacitação profissional; e 5. dimensão internacional.

No item “confiança no ambiente digital”, a estratégia brasileira aposta no estabelecimento de mecanismos de cooperação com empresas privadas e governos para uma melhor resposta a incidentes de segurança. A mesma lógica serve ao item “dimensão internacional”, no qual o Brasil deve participar de iniciativas internacionais de integração para a economia digital. A lógica do documento como um todo é atender às demandas de mercado.

Outro documento importante a ser observado é a *Política Nacional de Segurança da Informação* (PNSI), instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL, 2018). A PNSI aborda a “soberania nacional” de maneira superficial, apenas mencionando que é um de seus princípios.

A PNSI declara como seus objetivos a proteção do Estado e dos indivíduos, assim como a segurança dos dados custodiados por entidades públicas, a segurança da informação das infraestruturas críticas e o tratamento das informações com restrição de acesso, dentre outros pontos.

A política de segurança da informação também tem uma *Estratégia Nacional de Segurança Cibernética* (E-Ciber), que foi aprovada pelo Decreto Nº 10.222, de 5 de fevereiro de 2020 (BRASIL, 2020). Na E-Ciber, a palavra “soberania” não é encontrada nenhuma vez. A estratégia é dividida em dois tipos de eixos: 1. Eixos de Proteção e Segurança (governança cibernética; prevenção e mitigação de

ameaças); e 2. Eixos Transformadores (dimensão normativa; dimensão internacional e parcerias estratégicas; pesquisa, desenvolvimento e inovação; e educação).

Complementarmente, a Instrução Normativa Nº 5, de 30 de agosto de 2021 (BRASIL, 2021), publicada pelo Gabinete de Segurança Institucional da Presidência da República, estabelece requisitos mínimos de segurança da informação para a utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. Nos seus artigos 17 e 18, há procedimentos sobre como realizar os tratamentos de informação, proibindo informações classificadas com grau de sigilo em ambientes de nuvem:

> *"Art. 17. Em relação ao **tratamento da informação** em ambiente de **computação em nuvem**, o órgão ou a entidade, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:*
>
> *I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;*
>
> *II - **informação classificada em grau de sigilo** e documento preparatório que possa originar informação classificada **não poderão ser tratados em ambiente de computação em nuvem**;*
>
> *[...]*
>
> *Art. 18. **Os dados, metadados, informações e conhecimentos** produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, **devem estar hospedados em território brasileiro**, observando-se as seguintes disposições:*
>
> *I - pelo menos **uma cópia atualizada** de segurança deve ser mantida em **território brasileiro;***
>
> *II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;*
>
> *III - a **informação com restrição de acesso** prevista na legislação e o documento preparatório não previsto no inciso II do caput art. 17, bem como suas cópias atualizadas de segurança, **não poderão ser tratados fora do território brasileiro**, conforme legislação aplicável; e*
>
> *IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto."*
>
> *(Ibid., grifo nosso)*

A IN nº 5 um quadro exemplificativo de tipos descritivos de informação:

Tabela 4 – Tipos descritivos de informação, segundo IN nº 5

ANEXO
QUADRO EXEMPLIFICATIVO DE TIPOS DESCRITIVOS DE INFORMAÇÃO

Tipo	Descrição	
1. OSTENSIVA	Transparência Ativa	
	Transparência Passiva	
2. SIGILOSA CLASSIFICADA EM GRAU DE SIGILO	2.1 Reservada - Prazo máximo de restrição de acesso de 5 anos	
	2.2 Secreta - Prazo máximo de restrição de acesso de 15 anos	
	2.3 Ultrassecreta - Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos o prazo total da classificação.	
3. SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA (As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	3.1 Sigilos Decorrentes de Direitos de Personalidade	
		3.1.1 Sigilo Fiscal
		3.1.2 Sigilo Bancário
		3.1.3 Sigilo Comercial
		3.1.4 Sigilo Empresarial
		3.1.5 Sigilo Contábil
	3.2 Sigilos de Processos e Procedimentos	
		3.2.1 Sigilo do Procedimento Administrativo Disciplinar em Curso
		3.2.2 Sigilo do Inquérito Policial
		3.2.3 Segredo de Justiça no Processo Civil
		3.2.4 Segredo de Justiça no Processo Penal
	3.3 Informação de Natureza Patrimonial	
		3.3.1 Segredo Industrial
		3.3.2 Direito Autoral
		3.3.3 Propriedade Intelectual de Programa de Computador
		3.3.3 Propriedade Industrial
4. PESSOAL	4.1. Pessoal - Prazo máximo de restrição de acesso 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas.	

Fonte: NI n º 5/2021 (BRASIL, 2021)

Na atual organização do Governo Federal do Brasil, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI) é responsável pelas regras dos processos internos ao governo e pelo funcionamento da máquina pública. No ministério, existe a Secretaria de Governo Digital (SGD), que trabalha para impulsionar a digitalização dos serviços públicos.

A SGD produz uma série de documentos e serviços importantes para o Estado, como a *Estratégia Nacional de Governo Digital*, a nova Carteira de Identidade Nacional, o sistema GOV.BR (para acesso a serviços públicos *online*), um Padrão Digital de Governo e a Infraestrutura Nacional de Dados (IND).

Em 26 de outubro de 2023, foi publicada a Portaria SGD/MGI nº 5.950, que estabelece um modelo de contratação de *software* e de serviços de computação em

nuvem para a administração pública federal. É por meio desta portaria que as empresas estatais Serpro e Dataprev estão montando a chamada “Nuvem de Governo”, também chamada de “nuvem soberana”. Na página da SGD, que explica o que é a “Nuvem de Governo”, encontramos a palavra “soberania”:

> ***Por que a nuvem de governo é importante?***
>
> ***Segurança:*** *Os dados do governo são sensíveis e precisam de um alto nível de proteção. A nuvem de governo permite um controle mais rigoroso sobre a segurança da informação.*
>
> ***Soberania:*** *Ao utilizar uma nuvem própria, o governo garante que os dados estejam armazenados em território nacional, o que pode ser importante para questões de soberania e independência tecnológica.*
>
> ***Conformidade:*** *A nuvem de governo pode ser configurada para atender a requisitos específicos de segurança e conformidade, como as normas de proteção de dados.* (BRASIL, 2025d)

Conforme o texto publicado na página *web* do Ministério, “soberania” seria o mesmo que “localização de dados”, o que significa manter um determinado conjunto de dados coletados dentro de um determinado território[9]. Sem dúvidas, a localização de dados é uma medida importante para garantir a soberania nacional. Dados hospedados em território nacional estão regulados pela legislação do país, o que permite a ação coercitiva do Estado para forçar o cumprimento da lei. Tal possibilidade não existe quando as informações estão sob jurisdição estrangeira.

No mundo da computação em nuvem, a mera localização de dados é insuficiente para garantir a soberania porque, a depender da arquitetura da rede que guarda e processa os dados, dos equipamentos selecionados e dos *softwares* utilizados nessas redes, os fornecedores das soluções podem ter acesso às informações que se pretende proteger.

Um dos argumentos de venda mais propagandeados pelas empresas de nuvem é a chamada “escalabilidade”. Isso quer dizer que o cliente pode ter sua própria estrutura de data center. Porém, em momentos de alta demanda, o cliente pode “escalar” o serviço para a nuvem do fornecedor. Dependendo de como o

9 NOTA DO AUTOR: O termo “localização de dados” não deve ser confundido com “residência de dados”. O primeiro se refere a manter os dados dentro de um determinado território. O segundo é qualquer lugar onde os dados estejam hospedados.

contrato foi feito, as “nuvens parceiras” podem estar fora do território nacional. Quando isso acontece, as informações são transferidas para fora do controle do Estado e não há como saber, de fato, se o parceiro seguirá as regras contratuais.

4.1. Soberania como oportunidade de negócios

O que deveria ser preocupação com a proteção de dados do Estado e dos cidadãos se tornou uma excelente oportunidade de negócios. A Associação Brasileira das Empresas de *software* (ABES) anunciou, em março de 2025, que um dos focos da entidade para os próximos três anos será a *soberania digital*.

> *“Defendemos e defenderemos um **posicionamento regulatório** e **geopolítico** pragmático e estratégico, que **valorize** o desenvolvimento da **tecnologia nacional**, ao mesmo tempo em que promova um ambiente de negócios aberto, que **não discrimine** ou imponha barreiras à **tecnologia estrangeira**”*. [Declaração de Andriei Gutierrez, Presidente da ABES] (ABES, 2025, grifo nosso).

A ABES é formada por mais de 2 mil empresas associadas, dentre elas praticamente todas as *Big Techs*. Por isso, nas palavras do presidente da associação, não se pode “discriminar tecnologia estrangeira”. O objetivo da ABES é ajudar seus associados a conseguir novos negócios, o que é legítimo dentro do capitalismo. O que chama a atenção é o peso do tema “soberania digital” como uma das duas metas principais na agenda de curto e médio prazo da organização (a outra meta é “inovação”).

O Estado saber se suas informações serão preservadas por um fornecedor de serviços é um exercício de fé. Fé no parceiro e no contrato. Para as consultorias de segurança da informação, o invasor quase sempre será um *cracker/hacker*. É raríssimo achar algum artigo em mídia especializada de algum analista levantando dúvidas sobre a confiança na empresa privada, que é contratada pelo cliente estatal.

Um dos principais tipos de ataque de violação de cibersegurança é chamado no mercado de *“Man-in-the-Middle”* (“homem no meio do caminho”, tradução livre). Ocorre quando um cibercriminoso se usa de recursos tecnológicos para interceptar dados entre duas partes. Há várias formas de perpetrar este tipo de ataque. O

invasor pode instalar um programa ou código malicioso entre os dois pontos que estão se comunicando, e pode fingir ser uma das partes legítimas.

Outro tipo de ataque cibernético bastante comum é chamado de *ransomware*, que consiste em um “sequestro” computacional. O invasor utiliza algum *malware* ou outro recurso para criptografar arquivos que estão em alguma máquina, preferencialmente servidores, e impede o acesso ao sistema ou às informações até que um resgate seja pago, quando supostamente serão novamente desbloqueadas.

O que impede que esses tipos de ataque sejam feitos pelo fornecedor de serviços para uma empresa pública? Espionagem industrial, motivações geopolíticas ou disputas comerciais poderiam gerar uma ação de retaliação ou mesmo de sabotagem partindo de um Estado estrangeiro, executado por meio das empresas multinacionais a ele subordinadas.

Em 2024, a Fundação Getúlio Vargas publicou o *Relatório de pesquisa: soberania digital: para quê e para quem? Análise conceitual e política do conceito a partir do contexto brasileiro.* O documento mostra que o conceito de soberania digital está em disputa. Não há consenso entre as autoridades da República brasileira sobre o que isso significa. A pesquisa resultou em variadas interpretações, narrativas que coexistem e uma difusão de perspectivas. As visões variam da segurança nacional aos aspectos legais, autodeterminação econômica (inclusive desenvolvimento tecnológico), proteção de direitos, capacitação dos cidadãos/usuários e comunidades e defesa de normas e valores sociais, como tradições locais (CAMELO, 2024, p. 14). A pesquisa mostra que quando alguém fala em “soberania digital”, cada gestor público entende à sua própria maneira..

4.2. A “Nuvem Soberana” do Serpro

Primeiramente, é necessário registrar que para escrever esta seção, o autor desta tese conversou informalmente com diversos funcionários de carreira do Serpro, que ajudaram a esclarecer pontos da história recente da empresa e os problemas como a chamada “Nuvem Soberana”, que está em fase de implementação. Não é possível revelar os nomes dos funcionários, pois como estão na ativa, temem sofrer algum tipo de retaliação profissional. Todas as informações

recebidas por meio dessas conversas e utilizadas neste trabalho foram ratificadas em pesquisas em fontes oficiais ou referenciadas em matérias jornalísticas factuais. O que não pode ser confirmado, foi descartado.

Nas duas primeiras décadas do século XXI, o Serpro foi referência internacional pelo uso de *software* livre, inclusive na infraestrutura de seus *data centers*. A maior parte das máquinas do Serpro rodavam dentro dos centros de processamento de dados da estatal e havia forte estímulo para a utilização de Linux e outras soluções livres e abertas. Com o Golpe de 2016, que derrubou a Presidenta Dilma Rousseff, acabou também o Comitê de Implementação de *Software* Livre do Governo Federal do Brasil (CISL), que durou entre 2003 e 2016. O que havia de soberania digital começou a ruir.

Em 2019, a estatal realizou um chamamento público para identificar provedores de serviços em nuvem nas modalidades Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e *Software* como Serviço (SaaS) interessados em, em regime de parceria de negócio, prover serviços na plataforma multinuvem (SERPRO, 2019).

Em março de 2020, o Serpro firmou sua primeira parceria decorrente deste chamamento público, com Amazon Web Services (AWS), no valor de R$ 71,2 milhões (CONVERGÊNCIA DIGITAL, 2020). Um detalhe importante é que o contrato foi assinado com Amazon Web Service Inc., empresa que está subordinada às leis do estado de Washington, nos EUA, conforme pode ser comprado com a Figura 14.

Figura 14 – Impressão de tela do Diário Oficial da União, em 23/03/2020

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 23/03/2020 | Edição: 56 | Seção: 3 | Página: 28

Órgão: Ministério da Economia/Serviço Federal de Processamento de Dados

EXTRATO DE CONTRATO DE PARCERIA Nº 76.043/2020 - UASG 806030

Processo Nº: 00232-2020. Contratante: SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO). Contratada: AMAZON WEB SERVICE, INC. Objeto: Parceria de negócio com provedor de serviços em nuvem nas modalidades Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). Fundamentação: Art 28, §3º, inciso II e §4º da Lei 13.303/2016. Vigência: 02/03/2020 a 01/03/2025. Valor: R$ 71.200.910,03. Data da Assinatura: 02/03/2020. Nota de Empenho: 2020NE000302.

Fonte: DOU, 2020.

URL: https://www.in.gov.br/web/dou/-/extrato-de-contrato-de-parceria-n-76.043/2020-uasg-806030-249306681

O dispositivo jurídico que permitiu ao Serpro justificar a contratação da Amazon Web Services foi o Art. 28 da Lei 13.303/2016, a Lei das Estatais:

> *Art. 28. Os **contratos com terceiros** destinados à prestação de serviços às empresas públicas e às sociedades de economia mista, inclusive de engenharia e de publicidade, à aquisição e à locação de bens, à alienação de bens e ativos integrantes do respectivo patrimônio ou à execução de obras a serem integradas a esse patrimônio, bem como à implementação de ônus real sobre tais bens, serão precedidos de licitação nos termos desta Lei, ressalvadas as hipóteses previstas nos arts. 29 e 30. [...]*
>
> *§ 3º São as **empresas públicas** e as sociedades de economia mista **dispensadas da observância dos dispositivos** deste Capítulo nas seguintes situações: [...]*
>
> *II - nos casos em que a escolha do parceiro esteja **associada a suas características particulares**, vinculada a **oportunidades de negócio** definidas e específicas, justificada a inviabilidade de procedimento competitivo.*
>
> (BRASIL, 2016, grifo nosso)

Em sequência, outras parcerias foram sendo assinadas, seguindo o mesmo modelo. Em 2021, a segunda parceria de nuvem foi firmada com a chinesa Huawei, no valor de R$ 23 milhões (SERPRO, 2021a). Na sequência, no mesmo ano, foram assinadas parcerias com a Microsoft, no valor de R$ 22,6 milhões (idem, 2021b), e com a Oracle, no valor de R$ 41,5 milhões (idem, 2021c). Por fim, em 2022, foi assinado um contrato com a IBM, no valor de R$ 40,3 milhões (CONVERGÊNCIA DIGITAL, 2022). No total, foram R$ 198,6 milhões em contratos com as *Big Techs*.

A ideia principal dessas parcerias era que o Serpro oferecesse os produtos e serviços das multinacionais aos seus clientes. De 2023 em diante, a estratégia foi sendo modificada. As parcerias seguiriam normalmente como foram pensadas. Porém, a ação principal do Serpro seria voltar a priorizar os seus próprios *data centers*, mas com as soluções de "nuvem soberana" de seus parceiros.

Nesse momento, há uma mudança no direcionamento da estatal. Antes, os serviços contratados pelos clientes do Serpro poderiam ficar nos *data centers* das *Big Techs*. Agora, a orientação é que os serviços fiquem dentro dos *data centers* do Serpro, que montou uma infraestrutura própria e adquiriu *hardwares* e *softwares* das multinacionais. Ressalte-se que o modelo anterior continua valendo, depende apenas da decisão de quem quiser contratar.

Em seu *site*, o Serpro dedica uma página para explicar o que é "Nuvem de Governo". O conteúdo é publicitário e não revela muitos detalhes técnicos dos produtos e serviços oferecidos. Promete "*Soberania para dados do poder público"* e *"infraestrutura em nuvem de gestão 100% nacional, hospedada nos centros de dados do Serpro, com garantia de soberania e privacidade dos dados, inclusive confidenciais e sigilosos" (SERPRO, [s.d.])*.

A propaganda afirma que o Serpro faz *"uma Nuvem de Governo para Governo em plena conformidade com as regulamentações nacionais e com elevados requisitos de segurança que conferem alto grau de proteção e controle sobre dados sensíveis de governo e cidadãos" (ibid.)*.

Ainda segundo o *site*, as vantagens para algum cliente migrar para a Nuvem de Governo seriam: 1. manutenção de dados sensíveis dentro das fronteiras nacionais; 2. ênfase na segurança e na governança dos dados; 3. ausência de riscos de privacidade relacionados à transferência internacional de dados; 4.

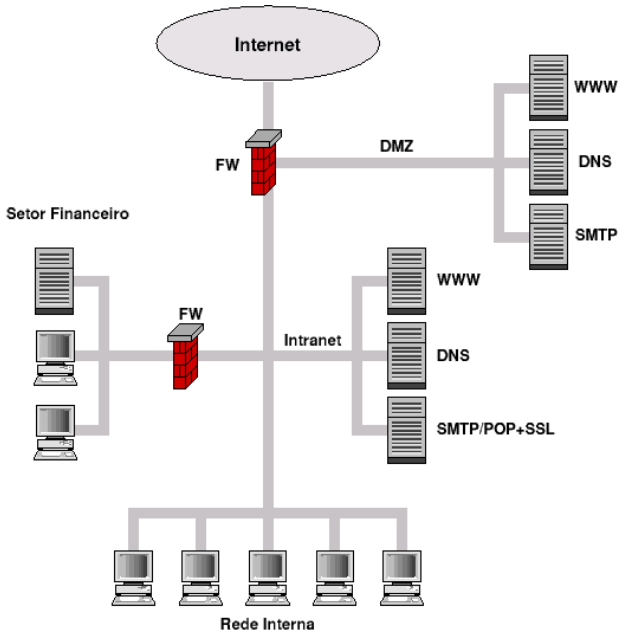
proteção contra ameaças cibernéticas; e 5. personalização da infraestrutura e suporte a aplicativos de alto desempenho.

Na mesma página, porém, mais adiante, quando pontua os “benefícios” da nuvem, afirma contar com *“resiliência e tolerância a falhas com oferta de multirregião”*. O Serpro não explica claramente como isso é feito, mas o que se entende no mercado como multirregião é a possibilidade de migrar dados para outros *data centers* selecionados, o que poderia significar a transferência de dados para instalações das *Big Techs*, mesmo que localizadas no Brasil.

Arquiteturas de TI e de segurança de rede podem ser montadas criando ambientes protegidos da Internet. Há várias formas de se fazer isso. Uma delas é colocar *appliances* (computadores pré-configurados e pré-montados para executar uma tarefa específica) na rede, inclusive para aplicações de inteligência artificial.

A Figura 15 ilustra como uma rede pode ser construída de forma que dados sensíveis fiquem apartados e mais protegidos. Saber exatamente como é montada a rede do Serpro é uma informação de segurança. Não revelar a infraestrutura é uma boa prática comum de segurança e de conformidade.

Figura 15: Exemplo de uso de firewall



Fonte: Cert.br. URL: https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html

Na hipotética figura 15, a Internet fica separada dos ambientes internos por *firewalls*, que são dispositivos de segurança que controlam o tráfego de rede, permitindo ou bloqueando o acesso. Na arquitetura desenvolvida no desenho, o "setor financeiro" (onde há dados extremamente críticos) é protegido por dois *firewalls*, enquanto na DMZ (área desmilitarizada, para interação com usuários externos), a Intranet e a rede interna são protegidas por apenas um *firewall*. O segundo firewall, que é um firewall interno, impede que até mesmo outros usuários dentro da rede acessem o "setor financeiro". Outras aplicações, como navegação na *web* (www), correio eletrônico (SMTP/POP+SSL) ou o Sistema de Nome de Domínio (DNS), podem ficar em camadas mais expostas.

As duas marcas de *firewalls* mais usadas no Serpro são a americano-israelense Check Point (www.checkpoint.com), com sedes em Tel Aviv e na Califórnia, e a marca norte-americana Palo Alto Networks, Inc. (paloaltonetworks.com), sediada também na Califórnia. Ambas as empresas são das mais respeitadas no mercado. Porém, as duas também precisam cumprir as leis dos Estados Unidos, como a CALEA, da qual trataremos com mais detalhes no capítulo 6. A CALEA exige que fabricantes insiram *backdoors* em seus dispositivos para permitir vigilância. Roteadores e *switches* são considerados equipamentos de comunicação e, portanto, estão diretamente submetidos à CALEA.

Um dos produtos que o Serpro está implementando dentro de sua infraestrutura é o Google Distributed Cloud Air-gapped. Essa solução, segundo definição da fabricante, é um ambiente de nuvem privada desconectada para gerenciamentos restritos, classificados ou ultrassecretos (GOOGLE, 2024). Assim, o Google promete que seus clientes, organizações do setor público, poderão atender às legislações nacionais, exigências regulatórias ou padrões de segurança. Esse modelo é chamado de *"Zero Trust"* (Confiança Zero, tradução livre).

No GDC Air-gapped tanto *hardwares* quanto *softwares* são fornecidos exclusivamente pelo Google. Não é possível comprar máquinas de outros fornecedores e nelas instalar o sistema Google. Isso torna bastante difícil ao cliente ter certeza quais operações aquela solução está realizando de fato.

Em síntese, o *Google Distributed Cloud Air-gapped* é apartado da nuvem pública do Google e roda inteiramente dentro do ambiente Serpro. Só que os

softwares e os *hardwares* (*appliances*) são do Google, que é uma empresa norte-americana. A saída para a Internet do *GDC Air-gapped* é protegida por camadas de segurança, sendo a técnica principal o uso de *firewalls*, que por sua vez também são fabricados por empresas de Israel ou dos EUA, cuja legislação (CALEA) exige que os fornecedores implementem *backdoors* em seus equipamentos.

Em artigo para o site da empresa Secureworks, Thomas Clements (2024) aponta como até mesmo ambientes *Zero Trust* estão sujeitos a falhas. Podem haver erros na hora da implementação do sistema, abrindo-se vulnerabilidades. Se não forem utilizados dispositivos com forte controle de segurança e acesso, credenciais podem ser roubadas. Técnicos descuidados podem se conectar a serviços externos por meio de dispositivos não confiáveis. Parte dos serviços pode, por diferentes razões, ser implementada sem dupla autenticação. Podem ocorrer ataques por Phishing (quando criminosos enganam a vítima para conseguirem senhas) ou do tipo *Man-in-the-Middle* (MitM). A segurança depende da forma como a solução é implementada e configurada e da qualidade da equipe envolvida. Roteadores e *switches* podem ser usados como portas de entrada para um ataque MitM.

Outro produto de “nuvem soberana” que o Serpro está implementando é o Amazon Web Services. Em 2023, a Amazon lançou uma solução de nuvem soberana para a Europa, que pretendia atender às regulamentações daquele continente, inclusive para o setor público, com residência de dados em territórios da Europa (AWS, 2023). Comentando sobre esse fato, Mikhail Korotaev escreveu um artigo listando argumentos do por que ele continuava a considerar a nuvem Amazon problemática para a soberania digital (KOROTAEV, 2023). Os principais pontos por ele elencados são:

- A Amazon tem características monopolistas, o que prende as administrações públicas em estruturas proprietárias controladas externamente;
- A Amazon tem controle exclusivo sobre suas tecnologias, o que limita a interoperabilidade com um ecossistema mais amplo;
- A dependência da Amazon significa fluxo contínuo de recursos financeiros da Europa para os Estados Unidos;

- Provedores de serviços passam a desenvolver novas soluções de acordo com o padrão Amazon, o que torna outras alternativas empresariais europeias menos atraentes ao cliente final;
- O código é fechado, não está disponível para revisão pública, não há garantia contra *backdoors* presentes nesses códigos ou que possam ser introduzidos por meio de atualizações e de correções de *software*;
- A Amazon tem o poder real de rescindir unilateralmente os contratos, se assim desejar;
- Clientes que dependem da Amazon podem ser forçados a pagar os preços que a empresa quiser praticar sob risco de descontinuidade dos serviços;
- A empresa pode mudar as regras de uso, e os seus clientes dependentes podem ter de flexibilizar regras de segurança de dados ou de independência das autoridades dos EUA.

Diferentemente do Google Distributed Cloud Air-gapped, a AWS não tem como ser uma solução totalmente apartada da nuvem Amazon. As instalações locais da AWS (*on-premisses*) são consideradas Zonas de Disponibilidade (AZ) da AWS. Se é uma AZ, ela necessariamente terá que ter conectividade redundante com outras regiões da AWS. Na página oficial do produto AWS Outposts, quando explica o que é necessário para fazer a instalação dos *hardwares*, está escrito que:

> ***Instalação***
>
> ***Rack do AWS Outposts***
> *A AWS oferece racks do Outposts totalmente montados e prontos para serem rolados para a posição final.* ***Os racks são instalados pela AWS*** *e* ***simplesmente*** *precisam ser* ***conectados à energia*** *e à rede.*
>
> ***Servidores AWS Outposts***
> *A AWS fornece servidores Outposts diretamente para você, instalados por equipe local ou por um fornecedor terceirizado.* ***Uma vez conectado à sua rede****, a* ***AWS irá provisionar remotamente*** *recursos de computação e armazenamento.* (AWS, [s.d.], grifo nosso)

O que está acontecendo no Governo Federal é que os órgãos que já haviam colocado seus sistemas na nuvem AWS, para atender à Portaria SGD/MGI nº 5.950, estão aderindo ao AWS Outposts da *multicloud* do Serpro, mantendo a plataforma

Amazon, pois a migração para outro sistema é lenta, difícil e custosa. Alguns gestores preferem e defendem a continuidade da solução AWS e sequer cogitam uma migração.

4.3. Entrevista com o Presidente do Serpro sobre a Nuvem Soberana

O Diretor-Presidente do Serpro, Alexandre Amorim, concedeu entrevista ao portal Convergência Digital (GROSSMAN, 2025b), em 20 de fevereiro de 2025, para anunciar o acionamento da Nuvem Soberana do Governo brasileiro, a partir do mês de março do mesmo ano. Na matéria, ele anunciou investimentos de R$ 700 milhões e uma combinação da infraestrutura prévia do Serpro com a aquisição de equipamentos das maiores Big Techs do setor. Na entrevista, Amorim declara:

> *"É **como termos um ambiente** onde toda nossa informação está guardada **dentro de um cofre**, na verdade de vários cofres, **que só eu tenho a chave**, só eu sei os segredos que tem lá e só eu consigo acessar. A tecnologia desses cofres **não foi eu que desenvolvi**, mas consegui **comprar no mercado** a melhor tecnologia, a melhor estrutura e ela **agora é minha**. Tenho o **domínio da propriedade**, faço a transferência de tecnologia para saber usar todos os ferramentais que ela possui, e os dados que estão lá dentro **só eu consigo apertar o código para acessar** e trabalhar aquelas informações", disse Amorim. [em entrevista para] (GROSSMAN, 2025b, grifo nosso).*

Mesmo se considerarmos que a entrevista foi dada a um veículo de comunicação que tem por objetivo transmitir a notícia para um público não técnico, as declarações estão cheias de imprecisões e de problemas.

O primeiro ponto é o uso da palavra "cofre". É uma imagem ruim, mesmo como metáfora. Um cofre real é um objeto físico e estático. Depois de fabricado, o cofre sempre será igual. Cofres modernos podem receber recursos eletrônicos e sensores, mas ainda assim terão um número limitado de funções específicas. Além disso, o cofre não tem a capacidade de vasculhar em tempo real o conteúdo do que está dentro dele. Mesmo que coloquemos uma câmera no cofre, ela mostrará somente o que está dentro do cofre, e não o conteúdo dos objetos que estão ali guardados. Se tenho um livro dentro do cofre, com uma câmera, poderei verificar se o livro está lá ou não, mas não ler as páginas daquele livro na hora que desejar. Os sistemas de computação em nuvem têm a capacidade de consultar os dados

sempre que necessário, transferi-los, copiá-los e alterá-los. Além disso, os sistemas em nuvem podem ser modificados constantemente pelos seus fabricantes. Aliás, essa é uma das propagandeadas vantagens da nuvem. Melhorias e correções de segurança não precisam esperar o lançamento de uma nova versão do *software*. Elas são implementadas sempre que necessário, a critério do fornecedor.

O uso da metáfora “chave” também é problemático. No campo da Tecnologia da Informação, quando se fala em chave, geralmente se refere à criptografia. Não é possível saber como o Serpro usa criptografia dentro de sua arquitetura de rede por óbvias razões de segurança, mas sabemos que a empresa usa esse tipo de tecnologia no sistema de Imposto de Renda e em aplicações de certificação digital.

Com certeza, a criptografia é um recurso de segurança imprescindível atualmente, mas mesmo ela tem suas limitações. Quando um dado trafega por um ambiente de nuvem, mesmo que circule criptografado, em algum momento ele precisa ser aberto para que ocorra a leitura humana. Nesse momento, pode ser interceptado e capturado. Mesmo que esse tipo de interceptação não ocorra, a criptografia pode ser quebrada.

A eficácia da criptografia depende da segurança das chaves criptográficas. Há técnicas e algoritmos especializados em tentar quebrar alguns tipos de criptografia. Quando há dependência de terceiros, dificilmente se pode ter certeza de que um fornecedor não estabeleceu um controle paralelo das chaves criptográficas dentro do seu sistema de nuvem. Sistemas da Amazon costumam armazenar as chaves criptográficas dentro de sua própria estrutura.

Os Estados Unidos têm um controle severo sobre para quais países as tecnologias que usam criptografia podem ser exportadas. Documento do Departamento de Comércio (EAR Supplement No. 1 to Part 740) divide as nações em grupos que vão de restrições leves ("*relaxed*") até controle estrito ("*strict export control*"). Este último veta a exportação para países listados como apoiadores de terrorismo (USA, 2018). Criptografia, para os EUA, recebe tratamento equivalente à munição de armamento real.

Há várias formas de se tentar quebrar a criptografia de sistemas digitais. A primeira e mais conhecida é a chamada "força bruta". Como explicado no *site* da empresa de cibersegurança Avast, trata-se de um ataque no qual se tenta adivinhar

a senha ou o código de criptografia para revelar a informação protegida. Há softwares invasores que experimentam o maior número de combinações de senhas possível até que a certa apareça e abra o arquivo criptografado (MOLINARO, 2024).

Vernalha (2023) explica que as medidas de segurança cibernética vão além do uso de criptografia. Faz-se necessário observar uma série de fatores para garantir a proteção de dados e da privacidade. Há que se ter políticas e procedimentos técnicos bem definidos e seguidos fielmente pelos trabalhadores envolvidos no processo. Toda a infraestrutura cibernética precisa estar protegida pelo uso de *firewalls*, sistemas de detecção e prevenção de intrusões e sistemas de autenticação forte. *Softwares* devem estar atualizados para corrigir vulnerabilidades conhecidas. A criptografia deve proteger não somente arquivos, mas dados em repouso e em trânsito, o que inclui a criptografia de disco, a criptografia de comunicação e a criptografia de dados confidenciais.

Outro problema para o uso de criptografia, no longo prazo, é a possibilidade da entrada de computação quântica no cenário tecnológico. Apesar de não estar madura o suficiente para ser comercializada em larga escala, empresas e universidades pelo planeta realizam pesquisas e testes com esse novo tipo de tecnologia. Os analistas mais otimistas acreditam que já haverá aplicação comercial em 2030, enquanto os pessimistas dizem que somente depois de 2040. No entanto, aplicações para uso da administração pública devem ser pensadas para que possam sobreviver em um horizonte temporal mais longo.

Retomando a entrevista com o Presidente do Serpro, Alexandre Amorim, no trecho em que ele diz: *“consegui comprar no mercado a melhor tecnologia, a melhor estrutura e ela agora é minha”*. A afirmação é equivocada. As parcerias a que ele se refere são com as *Big Techs*, especificamente Amazon (AWS), Google, Microsoft (Azure), Oracle e com a chinesa Huawei. Essas empresas não vendem a propriedade de seus sistemas, apenas concedem licenças de uso pelo tempo em que o contrato está ativo. No capítulo 5, teremos uma análise de algumas licenças e contratos do Serpro com essas multinacionais que mostrará como a declaração do presidente da estatal não condiz com a realidade.

Outro ponto da entrevista que gera dúvidas é quando o presidente diz que há “transferência de tecnologia”. Seria importante dizer qual o tipo. O Instituto Nacional

de Propriedade Intelectual (INPI) tem uma lista bem definida do que pode ou não ser considerado como transferência de tecnologia (BRASIL, 2017). A transferência de tecnologia que o Serpro está recebendo inclui Pesquisa & Desenvolvimento ou são apenas cursos e obtenção de certificações de mercado?

O que as empresas de Tecnologia da Informação costumam fazer é criar um conjunto de certificações e recomendar que as equipes técnicas de seus clientes as obtenham. A AWS, por exemplo, conta com pelo menos 12 exames de certificação. Os tipos de certificação abrangem *Cloud Computing*, Inteligência Artificial, *Machine Learning* e Segurança, entre outros (AWS, 2024a). Tirar essas certificações pode ser caro para um profissional autônomo, com preços variando entre US$ 100,00 e US$ 300,00 por certificado. Porém, as *Big Techs* fazem ofertas a preços especiais ou até mesmo gratuitas para clientes selecionados.

Quem trabalha com TICs geralmente aprecia a oportunidade de obter essas certificações, pois elas valorizam os currículos dos profissionais. Em alguns casos, agências de recrutamento e emprego preferem contratar profissionais com certificações avançadas a um diploma universitário.

Aprender novos conhecimentos sempre é desejável, mas a estratégia das *Big Techs* tem função dupla. Por um lado, essas empresas melhoram as capacidades da equipe técnica do cliente, o que permite que ela resolva uma série de problemas, sem a necessidade de acionar suporte técnico. Por outro, cria-se uma cultura de “fidelização” do cliente (ou aprisionamento), que sempre preferirá utilizar aquela tecnologia com a qual está acostumado ou certificado. O termo que o mercado usa para descrever esse processo é esclarecedor: “evangelização” da equipe de TI.

A fidelização da equipe, somada a tecnologias proprietárias, cria um efeito de vinculação do cliente com os fornecedores privados que, no longo prazo, torna-se muito difícil de ser quebrado. Um exemplo: bancos públicos e privados ainda utilizam a linguagem de programação COBOL, criada pela IBM, em 1959, porque as instituições financeiras dependem de um enorme legado de código COBOL acumulado por décadas. Não é simples reescrever essas aplicações e migrar para uma solução mais nova, sob pena de que um pequeno erro na transição poderia levar à perda de milhões de dólares, talvez bilhões.

A dependência de fornecedores de nuvem pode levar uma estatal, como o Serpro, a uma irrelevância funcional. Se os serviços oferecidos pela empresa são instâncias de soluções privadas, basta uma decisão de governo para que esses serviços sejam transferidos diretamente para as multinacionais. O pensamento dominante de parte das forças políticas no Brasil é o neoliberalismo, que tem nas privatizações um de seus pilares. Em democracias, quando ocorre alternância de poder, geralmente ocorrem mudanças de orientação governamental. Nesse contexto hipotético, o Serpro poderia ser vendido ou fechado.

Transferir o negócio principal (*core business*) para ambientes de nuvem das *Big Techs* poderia fazer da estatal uma mera revendedora de produtos de terceiros. Como empresa pública, o Serpro pode ser contratado diretamente, sem licitação, pela administração pública para prestação de serviços de Tecnologia da Informação. Dessa forma, há o risco de que, se algum órgão público quiser contratar um parceiro privado de nuvem, por qualquer razão, bastaria fazer um contrato com o Serpro e passar a usufruir do serviço da multinacional. É temerário que essa relação se transforme no que é popularmente chamado de “barriga de aluguel”, quando um ente público serve apenas para driblar a lei de compras do Estado. Não é objetivo desta tese fazer qualquer tipo de acusação; é apenas um alerta sobre a tênue camada que separa a relação público e privado.

A dependência de fornecedores privados pode colocar os órgãos públicos que contratam a estatal em uma posição de aprisionamento tecnológico (*vendor-lock-in*), que ocorre quando se fica preso a uma plataforma de *software*, tornando difícil ou custoso mudar para um concorrente.

O Serpro Multicloud obteve um recorde de novas contratações em 2024, aumentando em 64%, com clientes do poder judiciário, estados e municípios (alguns com mais de 250 mil habitantes). O Serpro se coloca como “*Cloud Broker*” (corretor de nuvem, tradução livre), oferecendo serviços AWS, Huawei, Microsoft, IBM, Google e Oracle. Matéria no *site* da estatal comemora o fato de que as compras possam ser feitas sem licitação:

> ***Acelere sua jornada para nuvem***
>
> *A migração de serviços públicos para nuvem é uma orientação vigente tanto em administrações públicas de outros países, como Estados Unidos e Reino Unido, quanto no Brasil. O Serpro apoia a adoção rápida e segura da tecnologia em nuvem, com a expertise de sua equipe técnica e a oferta de seus serviços especializados em nuvem.* ***O fato da contratação se dar por dispensa de licitação garante ainda celeridade*** *na melhoria do serviço e a continuidade do negócio. O Serpro Multicloud está disponível na loja da empresa pública do governo federal.*
>
> *(Serpro, 2025, grifo nosso)*

A demanda por novos contratos é favorecida pela recomendação do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) para que cerca de 250 órgãos do Governo Federal utilizem os serviços oferecidos pelo Serpro ou pela Dataprev, conforme publicado no site do ministério (BRASIL, 2024e).

Em abril de 2025, com um investimento de R$ 2,32 bilhões, ao longo de cinco anos, o Tribunal Superior do Trabalho (TST) e o Conselho Superior da Justiça do Trabalho (CSJT) firmaram um acordo institucional com o Serpro para o uso da solução Serpro Multicloud. A parceria estabelece um modelo de contratação unificado e escalável para toda a Justiça do Trabalho, incluindo os 24 Tribunais Regionais do Trabalho (TRTs), conforme matéria publicada pelo TI Inside (2025).

Na entrevista ao portal Convergência Digital (*sup. cit.*), o Diretor-Presidente Alexandre Amorim fala das vantagens da escalabilidade:

> *"Principalmente* ***a capacidade de expansão que as nuvens possibilitam****. Os sistemas estruturantes, eles têm uma escala que* ***do dia para noite eu tenho que crescer*** *porque tem uma* ***demanda*** *do Governo Federal ou de outro cliente: município, estado ou até mesmo de clientes privados. Então essa* ***elasticidade****, incorporar* ***Inteligência Artificial****, incorporar análises de dados, todas essas funcionalidades, as nuvens, elas já possuem"*
>
> *Alexandre Amorim In: (GROSSMAN, sup.cit., 2025, grifo nosso).*

No Brasil, há casos conhecidos de momentos de pico de demanda de processamento no setor público. São exemplos o último dia de entrega da declaração de Imposto de Renda, o processamento das provas do Exame Nacional do Ensino Médio (Enem) e a apuração das eleições brasileiras pelo Tribunal Superior Eleitoral (TSE). Na maior parte do ano, a infraestrutura do Estado é

suficiente para processar suas tarefas cotidianas. Porém, nesses momentos especiais, há um salto gigantesco de utilização.

O problema é que, ao escalar o processamento de dados para nuvens não controladas pelo Estado, perde-se o domínio sobre os dados sensíveis. Uma vez enviados, não se sabe o que o parceiro privado fará com aquelas informações.

O uso de Inteligência Artificial sem observar regras de segurança também pode ser uma ameaça à soberania digital. Quando alguém fizer uma consulta ao serviço de IA Generativa, a informação sai do ambiente controlado e vai para um servidor fora do Brasil. O pedido é processado e a IA retorna uma resposta ao usuário. No momento em que a informação é enviada para fora, não há mais certeza do que acontece com ela.

Sabemos que muitos programadores estão utilizando ferramentas de IA como Copilot, Gemini e ChatGPT-4 para acelerar processos de codificação de seus *softwares*. Quando se usa uma IA em nuvem para produzir esse tipo de conhecimento, expõe-se a regra de negócios do sistema que está sendo desenvolvido.

Uma empresa pode decidir usar uma IA intramuros, como a Vertex AI, criada para poder funcionar como uma IA apartada, oferecendo acesso aos modelos mais recentes do Gemini. Mas no caso do governo brasileiro, como essa IA seria alimentada? A Inteligência Artificial Generativa precisa de quantidades gigantescas de dados atualizados para que seja útil. Uma IA fechada dentro de um ambiente privado, que não melhora, terá pouca utilidade.

Por fim, no minuto 8:00 da entrevista, Amorim diz que *“[...] estaremos funcionando com tecnologia de ponta, a [mesma] que o governo norte-americano possui”*. Ora, isso não é uma vantagem. O Governo dos EUA não precisa espionar a si mesmo. As leis norte-americanas de espionagem são para vigiar países estrangeiros. As tecnologias digitais são aparatos de vigilância nunca antes vistas na História. Para tratarmos de soberania digital, este é o primeiro ponto que precisa ser compreendido pelos gestores públicos responsáveis.

CAPÍTULO 5
REGRAS PARA OS EXPORTADORES DE DADOS

Chamar de “exportadores de dados” as empresas que são clientes dos serviços de nuvem das *Big Techs* não é uma metáfora nem uma abstração. É um nome que a própria Microsoft utiliza em seus contratos e licenças, como veremos neste capítulo, mas que funcionaria para qualquer uma das outras empresas que oferecem esse tipo de serviço para o Serpro Multicloud.

Para entender melhor como ocorrem as parcerias entre a estatal Serpro e as grandes empresas provedoras de serviço de nuvem, o autor desta tese solicitou os contratos firmados via Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011). Porém, o Serpro negou o pedido, conforme a resposta abaixo:

> *“Em atendimento ao pedido de acesso à informação, o Serviço Federal de Processamento de Dados (Serpro) informa que não pode atender ao seu pedido, pois, os contratos em questão são sigilosos e se encontram protegidos pela legislação em vigor. Em particular, destacamos a Lei nº 12.527/2011 e o Decreto nº 7.724/2012, que definem as normas para o acesso à informação no âmbito da Administração Pública Federal.*
>
> *Conforme disposto no art. 23 da Lei nº 12.527/2011 e no art. 25 do Decreto nº 7.724/2012, não é permitido o acesso a informações sigilosas, que envolvam, por exemplo, segredos comerciais, industriais ou de negócios. Além disso, as informações são consideradas sigilosas em razão de legislação específica, nos termos do art. 22 da Lei nº 12.527/2011 e do art. 6º do Decreto nº 7.724/2012.*
>
> *Vale ressaltar que a divulgação de tais informações pode causar prejuízos à concorrência, gerando impactos negativos”.*
>
> *[Protocolo Fala.BR nº 18870.000575/2025-13 – Serpro, 2025]*

No entanto, o pesquisador Gabriel Boscardim de Moraes, integrante do Laboratório de Tecnologias Livres (LabLivre) da UFABC, para outra pesquisa, havia conseguido alguns contratos do Serpro com as *Big Techs*, ainda que a maior parte dos textos estivesse marcada com tarjas pretas que impediam a leitura. Os argumentos para a negativa parcial dos pedidos e para o tarjamento de informações foram *“existência de informações sigilosas”* ou *“desproporcionalidade do pedido”* (MORAES, 2024, p. 18).

Gabriel Moraes compartilhou os arquivos recebidos do Serpro, o que colaborou fundamentalmente com as análises que serão apresentadas a seguir. Apesar das várias informações omitidas, há trechos, principalmente quando são anexadas as licenças, que ajudam a provar como é a relação entre a estatal e as multinacionais. As licenças são parte integrante dos contratos.

Sendo assim, temos trechos legíveis dos contratos com as empresas Amazon, Huawei, IBM, Microsoft e Oracle, referentes ao chamamento público 1863/2019, feito para identificar provedores de Serviços em Nuvem nas modalidades Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e *Software* como Serviço (SaaS), para comporem a plataforma Serpro Multicloud.

Se somadas todas as páginas dos cinco contratos enviados pelo Serpro mais seus anexos, há mais de mil páginas de informação. Nesta seção, observaremos os pontos cruciais que, obviamente, não estão tarjados e que ajudam a comprovar o argumento desta tese. Muitas das regras impostas das *Big Techs* são similares de uma empresa para outra. Nesses casos, evitaremos repetições.

A Figura 16 é uma impressão de tela do *site* do Serpro, que apresenta os provedores de nuvem com quem a estatal trabalha.

Figura 16 – Provedores de nuvem do Serpro Multicloud

Fonte: SERPRO. URL: https://campanhas.serpro.gov.br/serpro-multicloud-

5.1. Contrato da Amazon com o Serpro

A solução Amazon que está sendo implementada pelo Serpro é o AWS Outposts. Segundo definição da fabricante, o AWS Outposts é uma forma de levar produtos, infraestrutura e modelos operacionais nativos da AWS para qualquer *data center*, espaço de colocalização ou instalações *on-premises*. São usadas as mesmas APIs, ferramentas e infraestruturas da AWS no local e na Nuvem AWS, em uma experiência híbrida. O AWS foi projetado para manter os ambientes do cliente e da Amazon conectados. Destaque para as palavras “híbrida” e ambientes “conectados”, o que mostra que a rede Serpro e a nuvem Amazon têm obrigatoriamente pontos de conexão, não estando 100% apartadas.

As cláusulas que serão avaliadas a seguir são integrantes do contrato CC EAWWPS00113710 2020 TR, de 20 de fevereiro de 2020, da Amazon Web Services, Inc. (sediada nos EUA) e da Amazon Web Services EMEA SARL (sediada em Luxemburgo) com o Serpro. Algumas são esclarecedoras dos riscos de soberania e de segurança para o ente público:

> *“3.2. **Privacidade de Dados.** O **Cliente poderá especificar as regiões AWS** nas quais o Conteúdo do Cliente será armazenado. O Cliente concorda com o armazenamento do Conteúdo do Cliente e com a **transferência** dele para as regiões AWS que o Cliente selecionar. **A AWS não terá acesso** ou usará o Conteúdo do Cliente **exceto** conforme necessário **para** manter ou oferecer as **Ofertas de Serviço**, ou conforme necessário para **cumprir com a lei ou com uma ordem** válida e vinculante **de uma entidade governamental** ou **regulatória**. A AWS não (a) divulgará o Conteúdo do Cliente para nenhum governo ou terceiros, ou (b) de acordo com a Cláusula 3.3., **deslocará o Conteúdo** do Cliente das regiões AWS escolhidas pelo Cliente **exceto**, em cada caso, conforme necessário **para cumprir com a lei** ou com uma **ordem** válida e vinculante **de uma entidade governamental** regulatória (como, por exemplo, uma intimação ou ordem judicial). Exceto se em violação a uma ordem judicial ou a outras exigências legais. A AWS notificará o Cliente com prazo razoável acerca de uma Notificação a respeito de qualquer determinação ou exigência legal de acordo com esta Cláusula 3.2, de modo que o Cliente possa pedir uma medida preventiva ou outro recurso jurídico adequado. A AWS usará somente as informações da Conta de acordo com a Notificação de Privacidade e o Cliente concorda com tal uso. **A Notificação de Privacidade não se aplica ao Conteúdo do Cliente.**”*
>
> *(Contrato AWS-Serpro. CC EAWWPS00113710 2020 TR, 2020, grifo nosso)*

“Regiões AWS” são áreas geográficas distintas onde a infraestrutura de servidores da AWS está localizada. Cada região é projetada para fornecer serviços de computação na nuvem com alta disponibilidade, baixa latência e redundância. Uma região é composta por várias Zonas de Disponibilidade (AZs), que são data centers fisicamente separados dentro da mesma área geográfica. Essa estrutura é criada dessa forma para se obter resiliência e tolerância a falhas. No site oficial da AWS, em “Infraestrutura global”, é possível verificar a relação de Regiões AWS e de AZs. Elas estão em todos os continentes, com mais presença na América do Norte e na Europa. Na América do Sul, a única Região AWS é São Paulo, responsável por locais de borda em todo o subcontinente: Rio de Janeiro, Fortaleza, Bogotá, Buenos Aires, Santiago e Lima (AWS, 2024b).

Como está claramente expresso na Cláusula 3.2, a Amazon não “acessará” ou “usará” o conteúdo do cliente EXCETO para manter ou estabelecer serviços ou para cumprir com as leis ou uma ordem vinculativa emitida por autoridades governamentais. Por ordem legal, a Amazon também pode transferir conteúdos das regiões AWS selecionadas pelos clientes. Ou seja, está escrito no contrato que a empresa tem o poder de acessar os dados do Serpro, se quiser ou precisar.

A Amazon Web Services, Inc. é uma empresa norte-americana, que obedece às leis do estado de Washington, nos EUA. Na Cláusula 12.5, está escrito que:

> *12.5.* ***Lei Aplicável; Foro. As leis do Estado de Washington, Estados Unidos,*** *sem referência a quaisquer normas de conflito de lei, regerão o presente Contrato e qualquer tipo de controvérsia que possa vir a surgir entre as partes. […] (Contrato AWS-Serpro, 2020)*

Na sequência, no item 12.6, o contrato estabelece que a solução Amazon está sujeita às leis e regulamentos de comércio norte-americanos, inclusive no que refere a sanções e boicotes internacionais.

> *12.6* ***Conformidade de Comércio.*** *No tocante ao presente Contrato, cada uma das partes* ***cumprirá com todas as leis e regulamentos*** *aplicáveis de controle de importação, reimportação, exportação e reexportação, sanções e boicotes,* ***incluindo todas as leis e regulamentos aplicáveis a empresas dos EUA****, tais como os Regulamentos de Administração da Exportação, os Regulamentos de Tráfico Internacional de Armas e os programas de sanções econômicas especificadas do país implementados pela Secretaria de Controle de Ativos Estrangeiros (OFAC). […] (Contrato AWS-Serpro, 2020)*

Continuando, na Cláusula 2.1, fica estabelecido que a Amazon pode interromper os serviços a qualquer tempo. Caso desejem descontinuar um serviço, basta avisar com 12 meses de antecedência. No entanto, se for por alguma questão urgente, como segurança da informação ou determinação legal, o serviço pode ser interrompido imediatamente.

> *2.* ***Alterações****.*
>
> *2.1.* ***Às Ofertas de Serviço. A AWS poderá****, de tempos em tempos, alterar ou* ***interromper*** *qualquer uma das Ofertas de Serviço. Para as Contas Empresariais da AWS cadastradas no Suporte da AWS no nível do Desenvolvedor ou acima (ou em qualquer serviço posterior que forneça alertas de comunicação)* ***a AWS notificará o Cliente****, com pelo menos* ***12 meses de antecedência****, caso a AWS decida interromper um Serviço disponibilizado a seus clientes em geral e que o Cliente esteja usando.* ***A AWS não será obrigada*** *a fornecer tal Notificação* ***se a interrupção for necessária*** *para endereçar uma* ***emergência*** *ou ameaça à segurança ou à integridade da AWS, responder reivindicações, lítigios ou perda de direitos de licença relativos a direitos de propriedade intelectual de terceiros, ou em cumprimento da lei ou atendimento de solicitações de uma entidade governamental. (Contrato AWS-Serpro, 2020)*

A Cláusula 6 dá direito à Amazon interromper o fornecimento dos serviços até que o cliente resolva o problema que motivou a suspensão temporário de acesso e de direitos de uso.

> *6.* ***Suspensão Temporária de Acesso e Direitos de Uso.*** *A AWS pode limitar temporariamente (total ou parcialmente, conforme estabelecido nesta Clásula 6) o direito do Cliente ou de qualquer Usuário Final de acessar ou usar as Ofertas de Serviços após uma Notificação ao Cliente [...] A AWS* ***restaurará*** *o acesso e uso do Cliente imediatamente o* ***após o Cliente ter resolvido o problema*** *que deu origem à limitação [...]. (Contrato AWS-Serpro, 2020)*

Mais à frente, de acordo com a Cláusula 7.2 (iii), a AWS poderá rescindir o contrato mediante notificação ao cliente com 90 dias de antecedência. Na Cláusula 7.3 (b) – *Recuperação do Conteúdo Pós-Rescisão*, a Amazon diz que não tomará nenhuma medida para remover o conteúdo do cliente nesses 90 dias. Depois desse período, o Cliente encerrará todas as Contas Empresariais da AWS. Isso significa que conteúdos hospedados e não migrados na AWS serão perdidos. Para o serviço público brasileiro, fazer uma migração em três meses pode ser pouquíssimo tempo e colocar em risco o atendimento à população.

Já a Cláusula 8.4 – *Sugestões*, fica acordado entre as partes que sugestões fornecidas pelo cliente à AWS poderão ser usadas pela empresa norte-americana sem restrições. Diferentemente do que ocorre com as comunidades de *software* livre, onde o esforço do trabalho coletivo é compartilhado com todos, no caso da AWS, os funcionários do Serpro poderão ter ideias que, se incorporadas, ajudarão somente o lucro da Amazon.

5.2. Contrato da Microsoft Azure com o Serpro

O Serpro apresentou dois arquivos digitais como parte do contrato com a Microsoft. O primeiro é o contrato de parceria em si. O segundo são anexos ao contrato. Ambos os documentos têm vários trechos tarjados de preto. Nos anexos há documentos-padrão da Microsoft, como o Contrato *Business and Services* e o Contrato *Enterprise*, além de regras para Registro para Servidor e Nuvem e Emendas aos Documentos do Contrato, dentre outros. O contrato é assinado com a Microsoft Corporation, sediada nos EUA, mas também com a Microsoft Brasil, cujo endereço é de São Paulo-SP. O contrato é regido pela lei brasileira (Cláusula 24). Não há um número específico de identificação do contrato, mas a data de assinatura é de 21 de maio de 2021. Pode ser rescindido entre as partes por conveniência (com 90 dias de antecedência) ou por justa causa (com 30 dias de antecedência).

Dos pontos que mais chamaram atenção, na Cláusula 14 – *Rede e Conexão*, mostra-se claramente como a rede Serpro deve ser conectada com os servidores da Microsoft para que possam funcionar corretamente:

> *"Salvo se de outro modo acordado por escrito entre as Partes, o SERPRO: (a) deve garantir que sua rede e sistemas cumpram as especificações relevantes (se houver) fornecidas por nós de tempos em tempos; (b) é o único responsável por adquirir e manter suas conexões de rede e links de telecomunicações de seus sistemas para os nossos data centers ou os de terceiros […]" (Contrato Microsoft-Serpro, 2021)*

A Cláusula 20 – *Da Proteção de Dados Pessoais* estabelece que a parceria entre o Serpro e a Microsoft deve cumprir a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018). Contudo, conforme o item (iii), fica acordado que, apesar de tanto o Serpro quanto a Microsoft serem operadores de dados dos clientes, cabe à estatal a responsabilidade de obter o consentimento de seus contratantes, majoritariamente órgãos públicos, para o tratamento de dados.

> *"(iii). com relação ao conteúdo dos clientes do SERPRO, ambas as Partes serão operadores de dados, devendo para tal, quando não houver outra base legal para tratamento de dados que o SERPRO obtenha expressamente, junto aos seus clientes, o consentimento necessário para o seu tratamento, de forma expressa e inequívoca". (Contrato Microsoft-Serpro, 2021)*

Além da obrigatoriedade de se cumprir a LGPD, no Anexo 3 – *Termos do Regulamento Geral de Proteção de Dados da União Europeia*, há regras para o cumprimento do Regulamento Geral de Proteção de Dados (GDPR), que é uma legislação europeia, sob a qual o Serpro não está submetido. Isso ocorre porque os anexos são, em maioria, documentos-padrão. Como a Microsoft é obrigada a atender ao GDPR, a incumbência fica estendida também ao Brasil. Esse ponto não é ruim, acaba por dar um pouco mais de segurança ao cliente, ao menos documentalmente, mas mostra como contratos e licenças são aceitos com poucas adaptações para as características locais de cada território.

No anexo denominado *Business and Services*, em sua Cláusula 4. (b), está escrito que os dados coletados poderão ser transferidos pela Microsoft para *data centers* localizados nos Estados Unidos ou em outros países:

> *b. As informações pessoais coletadas de acordo com este contrato (1) poderão ser transferidas, armazenadas e processadas nos Estados Unidos ou em qualquer outro país no qual a Microsoft ou seus provedores de serviços mantenham instalações e (2) estarão sujeitas aos termos de privacidade especificados nos Direitos de Uso. (Contrato Microsoft-Serpro, 2021)*

No anexo chamado *Registro para Servidor e Nuvem Adendo – Adendo de Proteção de Dados dos Microsoft Online Services – Brazil Only – ID do Aditamento M728* está escrito como o Serpro deve se submeter a outras leis estrangeiras. Na seção *Termos de Proteção de Dados*, inclui-se a *California Consumer Privacy Act* (Lei de Privacidade do Consumidor da Califórnia – CCPA). E na subseção *Termos Gerais/Cumprimento das Leis*, fica estabelecido que:

> *"[...] O Cliente é responsável por responder a todas as solicitações de um terceiro relativas ao uso que ele faz de um Serviço online, como uma solicitação para retirar conteúdo de acordo com a Digital Millennium Copyright Act (Lei dos Direitos Digitais do Milênio) dos Estados Unidos ou outras leis aplicáveis." (Contrato Microsoft-Serpro, 2021)*

Por fim, no *Anexo 2 – As Cláusulas Contratuais Padrão (Processadores)*, chama a atenção a terminologia utilizada na Cláusula 4, "*Obrigações do exportador de dados"*, que é o Serpro, e na Cláusula 5, *"Obrigações do importador de dados"*, que a Microsoft. Não fica nenhuma dúvida de como se dá o fluxo de dados do Brasil para o exterior por meio dessas parcerias de nuvem.

> ***O exportador de dados concorda e garante:***
>
> *(a) que o processamento, incluindo a transferência em si, de dados pessoais foi e continuará sendo realizada de acordo com as provisões relevantes da lei de proteção de dados aplicáveis (e, se aplicável, foi notificado às autoridades relevantes do Estado Membro no qual o exportador de dados está estabelecido) e não viola as disposições relevantes do Estado;*
>
> *(b) que ele seja instruído e durante toda a duração dos serviços de processamento de dados pessoais instruirá o importador de dados a processar os dados pessoais transferidos somente em nome do exportador de dados e de acordo com a lei de proteção de dados aplicáveis e as Cláusulas;*
>
> *(c) que o importador de dados fornecerá garantias suficientes em relação às medidas de segurança técnicas e organizacionais especificadas no Apêndice 2 abaixo;*
>
> *(d) que, depois de avaliar os requisitos da lei de proteção de dados aplicáveis, as medidas de segurança são apropriadas para proteger dados pessoais contra destruição acidental ou ilícita ou perda acidental, alteração, divulgação ou acesso não autorizado, especialmente onde o processamento envolva a transmissão de dados por uma rede e contra todas as formas ilícitas de processamento e que essas medidas garantem um nível de segurança apropriado aos riscos apresentados pelo processamento e pela*

> *natureza dos dados a serem protegidos tendo em vista os avanços tecnológicos e o custo de sua implementação;*
>
> *(e) que garantirá a conformidade com as medidas de segurança;*
>
> *(f) que, se a transferência envolver categorias especiais de dados, o titular dos dados foi informado ou será informado antes, ou tão logo seja possível, sobre a transferência de seus dados a um país de terceiro que não fornece proteção adequada segundo a Diretiva 95/46/EC;*
>
> *[…] (Contrato Microsoft-Serpro, 2021)*

5.3. Contrato da Huawei com o Serpro

A chinesa Huawei é única empresa que não é norte-americana da lista de parcerias do Serpro *Multicloud*. A parceria com a Huawei Cloud é composta do contrato principal e mais seis anexos, sendo: *Anexo I – Política de Uso Aceitável; Anexo II – Declaração de Privacidade; Anexo III – Contrato de Nível de Serviço Huawei Cloud; Anexo IV – Huawei Cloud 2021 – Acordo de Parceria; Contrato de Cooperação com Parceiro de Solução da Huawei Cloud;* e *Contrato de Certificação da HCPN*. Todos os documentos estão tarjados em vários trechos. A assinatura do contrato é com a Huawei do Brasil Telecomunicações Ltda., com regência da Lei brasileira. A rescisão por conveniência é por meio de notificação com seis meses de antecedência. Se for por justa causa, com notificação de 30 dias de antecedência.

Muitas cláusulas são bastante similares às que estão previstas nos contratos com as outras *Big Techs*. Algumas frases foram claramente copiadas de um contrato de uma empresa para outra, tendo exatamente a mesma redação, mas não há como saber qual foi o original, provavelmente o mais antigo.

Na Cláusula 1.1 – *Direitos Concedidos*, fica bastante claro que a propriedade da solução não é do Serpro, mas que fica garantido o “direito não exclusivo, não sublicenciável e intransferível” de combinar serviços da Huawei com o Serpro Multicloud.

Na Cláusula 1.7 – *Sua rede e conexão*, o Serpro é o único responsável por cumprir especificações relevantes e por conectar redes e *links* de telecomunicações com a Huawei.

Na Cláusula 2.4 – *Localização dos Dados*, o Serpro autoriza a transferência internacional de dados para os locais que escolher.

No Anexo I, fica acordado que a Huawei poderá investigar qualquer violação da *Política de Uso Aceitável*, o que significa que, para isso, a empresa pode monitorar os dados que trafegam pelos Serpro.

No Anexo II – *Declaração de Privacidade*, na Cláusula 2. *"Como a Huawei Cloud processa os Dados Pessoais da Contratante"*, fica estabelecido como a empresa chinesa pode ou não utilizar os dados do Serpro. Há regras de quando as informações poderão ser repassadas da Huawei para terceiros:

> *A Contratada **não poderá divulgar os Dados Pessoais** da Contratante a terceiros, **exceto** nos seguintes casos:*
> *a) A divulgação ser **obrigatoriamente exigida** de acordo com as **leis e regulamentos aplicáveis**.*
> *b) Podemos divulgar os Dados Pessoais da Contratante dentro do escopo mais limitado, quando apropriado, para **proteger direitos ou propriedade** da Huawei Cloud, dos clientes da Contratada e do público. [...]*
> *c) A Contratada **poderá divulgar** os Dados Pessoais da Contratante para as **empresas associadas** da Contratada, afiliadas, provedores de serviços, subcontratados, parceiros ou sucessores, **a fim de permitir que os mesmos forneçam suporte** a transações, suporte a serviços ou suporte de segurança à Contratante. [...]*
> *d) Somente divulgamos os Dados Pessoais da Contratante na extensão permitida pelas leis e regulamentos aplicáveis e de acordo com a presente Declaração. Não fornecemos, vendemos nem alugamos os Dados Pessoais da Contratante para terceiros, a menos que seja permitido de outra forma pela Contratante ou especificado na presente Declaração.*
>
> *(Contrato Huawei e Serpro, Anexo II, 2021, grifo nosso)*

5.4. Contrato da IBM com o Serpro

O Contrato da IBM com o Serpro foi entregue em arquivo único, de 42 páginas, e, assim como no caso anterior, muitas de suas cláusulas são idênticas aos contratos com as demais *Big Techs*. Muitas das cláusulas estão tarjadas. O contrato principal é chamado de "Contrato de Parceria para SERPRO Multicloud" e há três anexos: *Anexo I – Contrato IBM Business Partner de Parceria Comercial; Anexo II – Contrato de Serviços em Nuvem;* e *Anexo III – Parceiro Comercial IBM*. O contrato é assinado com a IBM Brasil Indústria Máquinas e Serviços Ltda., localizada no Rio de Janeiro, sendo regido pela lei brasileira. Não foi encontrada nenhuma peculiaridade que diferencie o contrato da IBM das regras já comentadas anteriormente.

5.5. Contrato da Oracle com o Serpro

O Contrato de Parceria para Serviços de Cloud Nº 1361/2021, entre Serpro e Oracle, tem 678 páginas. Como em casos anteriores, o documento mãe tem várias cláusulas copiadas de outros contratos. Há muitas páginas tarjadas. O contrato foi celebrado com a Oracle do Brasil Sistemas Limitada, sediada em Brasília-DF. O contrato é regido pela Lei brasileira. No entanto, nos anexos, há vários documentos em inglês. Também não foi encontrada nenhuma peculiaridade que diferencie o contrato da Oracle com regras já comentadas anteriormente.

5.6. Termos específicos de serviço do Google Distributed Cloud air-gapped

O Google Distributed Cloud air-gapped é outra solução anunciada pelo Serpro que compõe o sistema multinuvem da estatal. No entanto, neste caso, não conseguimos obter nenhum contrato com o Serpro. Por tal razão, a análise será feita com base nos *Termos de Serviço* padrão, disponíveis para qualquer usuário.

O portal do Google dedica uma página onde apresenta todos os “Termos de Serviço” e políticas de produtos do Google Cloud (https://cloud.google.com/product-terms). São vários documentos que se complementam a partir da parte da solução que o usuário decidir adquirir. Há termos específicos para “Google Cloud Platform”, para “Serviços de implementação”, para “Cloud Identity”, “Apigee (gerenciamento de APIs)” e “Serviços de SecOps”, dentre outros.

O Google Distributed Cloud air-gapped é descrito pela fabricante como uma solução de isolamento físico que oferece uma nuvem totalmente gerenciada para organizações que devem ter separação completa para atender a requisitos regulatórios e de soberania rigorosos. O cliente pode hospedar, controlar e gerenciar a infraestrutura e os serviços diretamente em suas instalações. No entanto, o Google oferece, opcionalmente, o serviço de *backup* em data centers multizona.

Observando o que está nos *Termos de Serviço* do Google Distributed Cloud air-gapped, versão de 21 de outubro de 2024, que só está disponível em língua inglesa (GOOGLE CLOUD, 2024), logo no primeiro item (*1. software terms*), verifica-se que o documento já deixa muito claro que o usuário não tem propriedade sobre

os programas computacionais ou equipamentos que compõem a solução. As licenças são não-exclusivas, não sublicenciáveis e não-transferíveis:

> *[1. software Terms] a. License. Google grants Customer* ***a non-exclusive, non-sublicensable, non-transferable license*** *during the Subscription Term to use the software ordered by Customer on Customer* ***Systems or hardware*** *only in accordance with (i) the Agreement and (ii) if applicable, the Scope of Use. […] (Ibid., grifo nosso)*[10]

No subitem ‘j’, o Google exige a destruição das cópias em caso de término de contrato de subscrição das licenças:

> *j. Termination. On termination or expiration of the Subscription Term, Customer will stop using all software and delete all copies. (Ibid.)*[11]

O subitem ‘c’, os *Termos de Serviço* apresentam a possibilidade de haver coleta e processamento de dados do cliente pelo Google, sendo que, nesses casos, há uma documentação especial detalhando o procedimento:

> *c. Documentation. Google may provide Documentation describing the appropriate operation of the software, including a description of how software is properly used, and* ***whether and how the software collects and processes data.*** *Customer will comply with any restrictions in the Documentation regarding software use. (Ibid., grifo nosso)*[12]

Já no subitem ‘d’, o Google reserva-se o direito de auditar periodicamente seus clientes para verificar se o uso da solução está em conformidade com o contrato. Mais do que isso, o cliente deverá prestar a assistência necessária para que a *Big Tech* possa realizar esse procedimento:

---

10 Tradução livre: [1. Termos do *software*] a. Licença. O Google concede ao Cliente uma licença não exclusiva, não sublicenciável e intransferível durante o Prazo da Assinatura para usar o *software* solicitado pelo Cliente em Sistemas ou *hardware* do Cliente somente de acordo com (i) o Contrato e (ii) se aplicável, o Escopo de Uso. [...]

11 Tradução livre: j. Rescisão. Na rescisão ou expiração do Prazo de Assinatura, o Cliente deixará de usar todo o *software* e excluirá todas as cópias.

12 Tradução livre: c. Documentação. O Google pode fornecer Documentação descrevendo a operação apropriada do *software*, incluindo uma descrição de como o *software* é usado corretamente e se e como o *software* coleta e processa dados. O Cliente cumprirá quaisquer restrições na Documentação sobre o uso do *software*.

> *d. Compliance With Scope of Use. As described in the Agreement, Customer will provide a sufficiently detailed written report describing its usage of each software product used by Customer and its software Users during the requested period (including as it relates to the applicable Scope of Use). If requested, Customer will provide reasonable assistance and access to information to verify the accuracy of Customer's software usage report(s).* ***Google reserves the right to periodically audit Customer to ensure Customer's compliance*** *with the Scope of Use and the terms of this "software Terms" section. (Ibid., grifo nosso)*[13]

No subitem "h", o documento coloca que o Google tornará disponíveis todas as cópias das versões atualizadas e melhorias de *software*. Os clientes deverão baixar e instalar as novas versões em até 30 dias. Isso significa que alterações de sistemas feitas pela multinacional precisam ser implementadas em pouquíssimo tempo pelos clientes, que quase não terão tempo para avaliar as modificações. Como há muito código-fonte proprietário e fechado na solução Google, fica quase impossível saber o que foi realmente feito dentro daquele bloco de código. O Google vende uma "caixa-preta" e demanda a instalação no ambiente do cliente dentro do prazo de um mês:

> *h.* ***Updates and Maintenance.*** *During the Subscription Term, if Customer is not purchasing GDC air-gapped on a Google-operated model, Google will make available to Customer copies of all current versions, updates, and upgrades of software, promptly upon general availability, as described in the Documentation. Google will notify Customer of each new release of the software and Customer is required to* ***download and install each new release within 30 days*** *of such notice. […] (Ibid., grifo nosso)*[14]

Um risco muito grave de se atualizar códigos-fonte sem possibilidade real de auditoria é a implantação pelo fornecedor de uma *"kill switch"* (interruptor de segurança, tradução livre). Esse debate foi reacendido pela guerra da Rússia contra

13 Tradução livre: d. Conformidade com o Escopo de Uso. Conforme descrito no Contrato, o Cliente fornecerá um relatório escrito suficientemente detalhado descrevendo seu uso de cada produto de *software* usado pelo Cliente e seus Usuários de *software* durante o período solicitado (incluindo no que se refere ao Escopo de Uso aplicável). Se solicitado, o Cliente fornecerá assistência razoável e acesso a informações para verificar a precisão dos relatórios de uso do *software* do Cliente. O Google reserva-se o direito de auditar periodicamente o Cliente para garantir a conformidade do Cliente com o Escopo de Uso e os termos desta seção "Termos do *software*".

14 Tradução livre: h. Atualizações e Manutenção. Durante o Prazo de Assinatura, se o Cliente não estiver comprando o GDC air-gapped em um modelo operado pelo Google, o Google disponibilizará ao Cliente cópias de todas as versões atuais, atualizações e upgrades do *software*, imediatamente após a disponibilidade geral, conforme descrito na Documentação. O Google notificará o Cliente sobre cada nova versão do *software* e o Cliente deverá baixar e instalar cada nova versão dentro de 30 dias de tal notificação. [...]

a Ucrânia, em especial após a aproximação do Presidente Donald Trump com Vladimir Putin, no início de 2025. A Europa começou a repensar seriamente seu setor militar, em como se defender sem depender dos EUA. Um dos temores é a possível existência de uma "*kill switch*" em caças norte-americanos vendidos aos europeus, em especial o F-35 Lookheed (DESMARAIS, 2025).

Na área da computação, *"kill switch"* se refere a um mecanismo projetado para desativar ou desligar imediatamente um sistema, dispositivo ou software em caso de emergência ou de comprometimento. Não é difícil imaginar que, mesmo que o Google (ou qualquer outra empresa que comercializa *software* proprietário de código-fonte fechado) não tivesse acesso à infraestrutura do Serpro, ele simplesmente poderia implementar uma "*kill switch*" e incluí-la na sua mais recente atualização (se é que já não existe). Conforme a licença do Google Cloud, o cliente tem um mês para instalar a nova versão. Em um conflito hipotético do Brasil com os EUA, um ataque deste tipo poderia comprometer severamente a capacidade do poder público brasileiro de funcionar.

O marketing do Google vende a integração do sistema de nuvem com Inteligência Artificial como uma das principais vantagens competitivas para que o cliente resolva contratar o serviço. A seção 8 dos *Termos de Serviço* aborda a IA Generativa. No subitem "a", quando apresenta a definição, o documento já explica que o serviço de IA generativa usa dados do cliente para criar um determinado resultado. Significa que o sistema de IA do Google poderá acessar a base de seus clientes para coletar dados para processar uma resposta ao que lhe for solicitado.

> ***8. Generative AI Services.***
> *a. Definition. "Generated Output" means the data or content generated by a Generative AI Service prompted by* ***Customer Data****. Generated Output is Customer Data. As between Customer and Google, Google does not assert any ownership rights in any new intellectual property created in the Generated Output.*
> *(Ibid., grifo nosso)*[15]

15 Tradução livre: 8. Serviços de IA Generativa. a. Definição. "Saída Gerada" significa os dados ou conteúdo gerados por um Serviço de IA Generativa solicitados pelos Dados do Cliente. Saída Gerada são Dados do Cliente. Entre o Cliente e o Google, o Google não afirma nenhum direito de propriedade sobre nenhuma nova propriedade intelectual criada na Saída Gerada.

A fuga de dados por meio de sistemas de Inteligência Artificial preocupa alguns gestores públicos. Em 20 de março de 2025, o Conselho de Controle de Atividades Financeiras (COAF), órgão do Governo Federal, vinculado ao Banco Central do Brasil, expressou preocupação com o uso indevido de IA Generativa ao publicar no Diário Oficial da União a Portaria COAF nº 4 (BRASIL, 2025e).

No Art. 2º da Portaria foi proibido *"o tratamento de dados e informações sujeitos a regimes jurídicos próprios de sigilo, a exemplo dos relacionados à produção de inteligência financeira, fiscalização de pessoas obrigadas e proteção de dados pessoais sensíveis em plataformas externas de IAG" (Ibid.).*

O veto se aplica inclusive à plataforma Microsoft Copilot, com quem o COAF mantém um contrato de prestação de serviços ativo. Qualquer ferramenta de IA Generativa deverá ser previamente avaliada pelos servidores públicos responsáveis pela TI do órgão antes de ser utilizada em produção.

Retornando ao termo de uso do Google Cloud, o item 11. *Customer Security Measures* trata dos cuidados de segurança que os clientes devem ter ao usarem os serviços do Google Cloud. Fica declarado que apenas pessoas autorizadas podem ter acesso e manipular os *softwares* e modelos do Google. O cliente precisa implementar medidas que limitem acessos tanto físicos quanto por rede. Isso demonstra a possibilidade técnica dos sistemas serem acessados remotamente. Isso pode ocorrer por falhas ou erros de implementação de segurança. Dependendo da forma como a arquitetura de rede foi montada, tanto pessoas designadas pelo cliente, como funcionários da Google ou *crackers/hackers*, usando métodos lícitos ou não, podem conseguir entrar nos sistemas, apesar do Google Distributed Cloud air-gapped estar em rede apartada.

> *11.* ***Customer Security Measures.***
> *b. Digital Security Measures. Customer will ensure that reasonable digital security measures are implemented to ensure that only Designated Persons have access to copy, download, backup, write to, or modify software and Google Models. Such measures include, but are not limited to, digital access control, access logs, restrictions on the use of external storage devices, vulnerability scans, firewalls, and intrusion detection systems.*
> *(GOOGLE CLOUD, sup. cit., 2024.)*[16]

16 Tradução livre: 11. Medidas de Segurança do Cliente. b. Medidas de Segurança Digital. O Cliente garantirá que medidas razoáveis de segurança digital sejam implementadas para garantir que somente Pessoas Designadas tenham acesso para copiar, baixar, fazer backup, gravar ou modificar o *software* e os Modelos do Google. Tais medidas incluem, mas não estão limitadas a, controle de acesso digital, registros de acesso,

Por fim, no item 15. *Government Rights*, que aborda a relação do Google com governos, fica bem claro que o cliente governo tem os mesmos direitos fornecidos habitualmente a clientes comerciais e a ao público em geral, sem qualquer tipo de regime especial de tratamento:

> *15.* ***Government Rights****. [...] Except as may be otherwise agreed, any government rights related to GDC air-gapped* ***include only those rights customarily provided to commercial customers and the public as described in these Service Specific Terms or the Agreement.*** *No other rights in GDC air-gapped (including any related hardware, software, technology, machine learning models, and documentation) will be transferred to the government unless agreed in the Agreement or an amendment to the Agreement. [..]*
> *(Ibid., grifo nosso)*[17]

A 'Nuvem de Governo' do Serpro não pode ser considerada como produto ou serviço de soberania digital ou de dados por ser fortemente dependente de fornecedores estrangeiros, depender de infraestrutura híbrida de parceiros privados, haver a possibilidade de transferência de dados à revelia da autorização do poder público brasileiro, estar submissa à legislação estrangeira, poder ser desligada a qualquer tempo por razões contratuais, não deter a propriedade dos sistemas envolvidos, que devem ser destruídos ou ter seu uso interrompido em caso de fim de contrato. Os sistemas são fechados e não auditáveis, com risco de introdução de códigos que sirvam como um tipo de kill switch, incapacitando o funcionamento das soluções.

---

restrições ao uso de dispositivos de armazenamento externo, varreduras de vulnerabilidade, firewalls e sistemas de detecção de intrusão.

17 Tradução livre: 15. Direitos do Governo. [...] Exceto quando acordado de outra forma, quaisquer direitos governamentais relacionados ao GDC air-gapped incluem apenas aqueles direitos habitualmente fornecidos a clientes comerciais e ao público, conforme descrito nestes Termos Específicos de Serviço ou no Contrato. Nenhum outro direito no GDC air-gapped (incluindo qualquer *hardware*, *software*, tecnologia, modelos de aprendizado de máquina e documentação relacionados) será transferido ao governo, a menos que acordado no Contrato ou em uma emenda ao Contrato. [..]

5.7. Quadro-resumo

Tabela 5 – Riscos de soberania em contratos e licenças

Riscos de soberania de licenças e contratos do Serpro com as Big Techs / Termo padrão GDC	
• Dependência de fornecedor; • Nuvens híbridas com Big Techs; • Possibilidade da Big Tech transferir dados sem autorização; • Possibilidade técnica da Big Tech acessar ou usar dados do cliente; • Submissão a leis não brasileiras; • Estar sujeito a sanções internacionais ou participar delas; • Riscos de suspensão dos serviços; • Suspensão temporária de acesso e de direitos de uso; • Risco de não conseguir migrar conteúdos após término de contrato; • Sugestões e melhorias viram propriedade das Big Techs; • Mesmos direitos e deveres de qualquer cliente;	• Ônus de ser operador e responsável por dados dos clientes brasileiros hospedados em nuvens estrangeiras; • Risco de descumprimento da LGPD; • Não há propriedade dos sistemas por parte do cliente brasileiro, mas direitos de uso; • Sistemas de código fechado e não auditáveis. • Exigência de destruir cópias após término dos serviços; • Direito da Big Tech auditar o data center do cliente; • Atualização de software sem que se possa fazer auditoria e/ou em curto prazo; • Risco de implantação de Kill Switch; • Risco de fuga de dados para alimentar Inteligência Artificial.

Fonte: Elaborado pelo autor (CASSINO, 2025)

CAPÍTULO 6
DISPOSITIVOS DA LEGISLAÇÃO DOS EUA

As principais empresas fornecedoras de serviços de nuvem no Brasil são norte-americanas: Google, Amazon, IBM, Oracle e Microsoft. Das corporações que são parceiras do Serpro Multicloud, a única que não tem sede nos Estados Unidos é a chinesa Huawei. Esse fato faz com que a necessidade de observar a legislação dos EUA seja fundamental para entender os riscos de soberania digital envolvidos. Olhar a lei chinesa seria importante também, mas como a participação de mercado das empresas daquele país ainda são bastante minoritárias no ocidente, o foco ficou na avaliação das leis norte-americanas.

As leis em si não são garantia de nada, pois em um cenário geopolítico complexo, os Estados podem usar de recursos fora das legislações nacionais e dos acordos internacionais para praticar atos de vigilância, espionagem, sabotagem e guerra eletrônica. Tudo depende dos conflitos bélicos ou comerciais e da decisão executiva de acionar os dispositivos tecnológicos contra rivais ou parceiros-alvo.

As *Big Techs* sediadas nos Estados Unidos estão submetidas às leis norte-americanas e são obrigadas a cumpri-las. Principalmente após os ataques terroristas de 11 de setembro de 2001, os EUA ampliaram e aperfeiçoaram seus dispositivos legais para permitir a exigência de entrega de dados e informações por meio dessas companhias.

Os dispositivos da legislação norte-americana mais importantes no sentido de autorizar e forçar a captura de dados de terceiros são a FISA (1978), a CALEA (1994), a Patriot Act (2001), a Freedom Act (2015) e a *Cloud Act* (2018). Neste capítulo, destacaremos os pontos mais relevantes de cada um deles.

6.1. FISA – *Foreign Intelligence Surveillance Act* (1978)

De acordo com o *site* oficial INTEL.GOV ([s.d.]), mantido pela Comunidade de Inteligência dos EUA, a *Foreign Intelligence Surveillance Act* (FISA) (Lei de Vigilância de Inteligência Estrangeira, tradução livre), aprovada em 1978 pelo Congresso norte-americano, tem sido modificada ao longo dos anos para fornecer

ferramentas para a coleta de informação de inteligência estrangeira e para a proteção da privacidade e das liberdades civis.

A FISA regulamenta diversos tipos sensíveis de atividades de coleta de inteligência que ocorrem dentro do país. Para vigilância eletrônica contra alguém presente no território dos EUA, o Governo deve ter uma ordem do Tribunal de Vigilância de Inteligência Estrangeira (FISC). Para obter tal ordem, é necessário demonstrar as razões da suspeita, de forma semelhante à obtenção de autorização para grampos telefônicos.

Porém, um dos pontos mais relevantes da FISA, em sua seção 702, é a permissão ao Governo para compelir empresas norte-americanas a colaborar na identificação de não-americanos localizados fora dos EUA para a coleta de informações de inteligência (dados e metadados). Para esses casos, nenhuma autorização do Tribunal é necessária, sendo exigido apenas o cumprimento de procedimentos bem definidos.

> *(5) Enforcement of directives. (A) Order to compel.--If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.*
> *(FISA, Sec. 702, 2008)*[18]

Esse trecho da FISA elimina qualquer tipo de dúvida sobre a capacidade legal e técnica do governo norte-americano de agir caso uma empresa provedora de serviços eletrônicos não cumpra o disposto na lei.

Exemplos de como a Seção 702 da FISA é usada em operações eletrônicas podem ser encontrados no *site* do Federal Bureau of Investigation (FBI, 2023). Conforme relato de 1º de dezembro de 2023, o FBI relata sucesso na identificação dos esforços de *hackers* da República Popular da China contra um centro de transportes nos EUA. Outro caso envolve *hackers* iranianos que monitoravam um

18 Tradução livre: (5) Aplicação de diretivas. (A) Ordem para obrigar. Se um provedor de serviços de comunicação eletrônica não cumprir uma diretiva emitida de acordo com o parágrafo (1), o Procurador-Geral pode apresentar uma petição para uma ordem para obrigar o provedor de serviços de comunicação eletrônica a cumprir a diretiva com o Tribunal de Vigilância de Inteligência Estrangeira, que terá jurisdição para revisar tal petição. (FISA, Sec. 702, 2008)

ex-funcionário do FBI, permitindo que a pessoa-alvo fosse avisada e tomasse medidas para proteger sua própria segurança.

Um boletim do Gabinete do Diretor de Inteligência Nacional, também de 2023, divulga o uso da Seção 702 da FISA para monitorar atividades russas na guerra contra a Ucrânia, identificar a fonte de múltiplos ataques de *ransomware* praticados por estrangeiros contra infraestruturas críticas dos EUA e procurar atividades terroristas ou o recrutamento de espiões por outras nações para atuação em solo norte-americano (USA, 2023b).

6.2. CALEA – *Communications Assistance for Law Enforcement Act* (1994)

Apenas a FISA já dá poder às autoridades norte-americanas para que obtenham os dados e as informações sob posse das empresas de Tecnologia da Informação. Porém, a *Communications Assistance for Law Enforcement Act* – CALEA (Lei de Auxílio das Comunicações para a aplicação do Direito, tradução livre), aprovada em 1994, exige mudanças nos projetos de *hardware* e de *software* para que a vigilância seja permitida (USA CALEA Act, 1994).

De início, a CALEA servia apenas à vigilância de redes telefônicas. Após 2005, foi alterada para permitir o monitoramento de Voz sobre IP (VoIP) e de tráfego de dados via conectividade banda larga à Internet.

A CALEA impõe que operadoras de telecomunicações e que fabricantes de equipamentos modifiquem e projetem *hardwares*, instalações e serviços para facilitar as ações de vigilância do poder estatal. A lei permite que a operadora desenvolva sua própria solução ou compre de terceiros. Exige também que as operadoras tenham um Plano de Segurança e Integridade do Sistema (SSI), que deve ser atualizado com frequência, informando as modificações à Comissão Federal de Comunicações (FCC).

A lei explicita que os provedores de serviços de comunicação devem auxiliar as autoridades policiais na realização de vigilância de comunicações, seja por telefone ou por rede de computadores. Isso inclui informações, instalações e assistência técnica para realizar as interceptações (USA, 2025).

Conforme pode ser lido em resumo publicado no portal do Congresso norte-americano (USA, 1994), as empresas devem permitir que o Governo intercepte todas as comunicações eletrônicas simultaneamente à sua transmissão ou em qualquer momento posterior, desde que aceitável para o poder público.

A entrega de informações deve ser em formato acessível ao ente governamental. Na Seção 106, há a exigência de que os fabricantes de equipamentos de transmissão ou comutação de telecomunicações e os provedores de serviços de suporte de telecomunicações disponibilizem às operadoras os recursos ou modificações necessários para permitir o cumprimento da lei.

> ***(a) CONSULTATION -*** *A telecommunications carrier shall consult, as necessary, in a timely fashion with manufacturers of its telecommunications transmission and switching equipment and its providers of telecommunications support services for the purpose of* ***ensuring that current and planned equipment, facilities, and services comply with the capability*** *requirements of section 103 and the capacity requirements identified by the Attorney General under section 104.*
>
> ***(b) COOPERATION -*** *Subject to sections 104(e), 108(a), and 109 (b) and (d), a manufacturer of telecommunications transmission or switching equipment and a provider of telecommunications support services shall, on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its equipment, facilities, or services such features or modifications as are necessary to permit such carriers to comply with the capability requirements of section 103 and the capacity requirements identified by the Attorney General under section 104.*
>
> *(USA CALEA Act, Sec. 106, 1994)*[19]

19 Tradução livre: (a) CONSULTA - Uma operadora de telecomunicações deve consultar, conforme necessário, em tempo hábil, os fabricantes de seus equipamentos de transmissão e comutação de telecomunicações e seus provedores de serviços de suporte de telecomunicações com o propósito de garantir que os equipamentos, instalações e serviços atuais e planejados estejam em conformidade com os requisitos de capacidade da seção 103 e os requisitos de capacidade identificados pelo Procurador-Geral sob a seção 104 (b) COOPERAÇÃO - Sujeito às seções 104(e), 108(a) e 109 (b) e (d), um fabricante de equipamentos de transmissão ou comutação de telecomunicações e um provedor de serviços de suporte de telecomunicações devem, em tempo hábil e a um custo razoável, disponibilizar às operadoras de telecomunicações que usam seus equipamentos, instalações ou serviços, tais recursos ou modificações conforme necessário para permitir que tais operadoras cumpram os requisitos de capacidade da seção 103 e os requisitos de capacidade identificados pelo Procurador-Geral sob a seção 104. (USA CALEA, Sec. 106, 1994)

Recentemente, devido às crescentes tensões entre Estados Unidos e República Popular da China, pesquisadores, políticos e ativistas começaram a tecer novas críticas à CALEA. Um dos principais argumentos é que as *backdoors* que permitem ao Governo norte-americano promover vigilância também poderiam ser utilizadas por agentes estrangeiros para atacar sistemas dos EUA (LANDAU, 2024).

6.3. *Patriot Act* (2001) e *Freedom Act* (2015)

Após 11 de setembro de 2001, quando dois aviões atingiram as Torres Gêmeas do World Trade Center, em Nova Iorque, outro foi lançado contra o Pentágono, em Washington DC, e uma última aeronave caiu cheia de passageiros, com todos os incidentes resultando em quase três mil mortos, os EUA deflagraram sua Guerra ao Terror.

Dentre as respostas aos ataques e para prevenir ameaças futuras, entrou em vigor a *Patriot Act* (Lei Patriota, tradução livre). A nova legislação foi usada para uma série de operações supostamente antiterroristas. Porém, conforme publicação do Departamento de Justiça dos EUA, a *Patriot Act*, com o tempo, começou a ser usada para combater o crime comum, como tráfico de drogas (USA, [*s.d.*]).

O objetivo principal da lei é permitir ao Estado ações de vigilância para antecipar-se a ameaças ao povo norte-americano, o que inclui o uso de grampos telefônicos e vigilância de comunicação eletrônica. Na verdade, a *Patriot Act* atualizou as formas de utilização das novas tecnologias digitais para as investigações. Pessoas vítimas de ataques *crackers/hackers* passaram a poder solicitar ajuda policial contra os cibercriminosos. A vigilância eletrônica equiparou-se a ações de vigilância física. A lei também facilitou o compartilhamento de informações entre as agências de segurança e de inteligência dos EUA, como o FBI, a CIA e a NSA. As pessoas e instituições alvo de vigilância passaram a poder ser espionadas sem que fossem avisadas previamente.

Em 2015, várias provisões da *Patriot Act* estavam prestes a expirar, o que levou a uma reforma de vários de seus dispositivos. O texto legal foi chamado de *Freedom Act* (Lei da Liberdade, tradução livre). Algumas mudanças foram introduzidas, que, ao menos legalmente, melhoraram um pouco o direito à

privacidade e as liberdades civis do povo norte-americano, como a limitação da coleta em massa de metadados de telefonia (USA FREEDOM Act, 2015).

6.4. *Cloud Act* (2018)

Com a popularização da Computação em Nuvem, o legislativo dos EUA se mobilizou para aprovar, em 2018, uma regulamentação sobre esse tema: a *Clarifying Lawful Overseas Use of Data Act* (Lei de Esclarecimento do Uso Legal de Dados no Exterior, tradução livre). Ou, simplificadamente, *Cloud Act* (Lei da Nuvem).

A lei altera o código penal para que um provedor de serviço de comunicação eletrônica ou serviço de computação remota cumpra com os requisitos para preservar, fazer cópia de segurança (*backup*) ou divulgar o conteúdo de uma comunicação eletrônica, registros ou informações não relacionadas a conteúdos pertencentes a um cliente ou assinante, independentemente de a comunicação ou registro estarem localizados dentro ou fora dos Estados Unidos.

A *Cloud Act* oferece às empresas formas de contestar pedidos de divulgação de conteúdo em certos casos, a depender da nacionalidade ou residência do cliente ou assinante. Também podem apelar caso a divulgação exigida crie um risco material de que o provedor viole as leis de um governo estrangeiro com o qual os Estados Unidos tenham em vigor um acordo executivo sobre acesso a dados. O Brasil, por exemplo, tem com os EUA um Tratado de Assistência Jurídica Mútua (MLAT) em vigor desde 2001. Em todos os casos, a palavra final será da Justiça norte-americana.

A lei também prevê como deve ser a resposta das empresas caso a ordem de acesso venha de um governo estrangeiro. Nesses casos, os provedores podem: interceptar ou divulgar o conteúdo de uma comunicação eletrônica, divulgar o conteúdo de uma comunicação eletrônica armazenada, ou divulgar registros e informações não relacionadas a um assinante ou cliente.

Não é objetivo da lei impedir que uma autoridade estrangeira obtenha assistência em investigações criminais. A *Cloud Act* estabelece uma estrutura para facilitar que os EUA celebrem acordos executivos com governos estrangeiros para acesso a dados e sobre privacidade. Esses acordos viriam para prevenir conflitos

legais entre autoridades demandantes e países onde as empresas de nuvem guardam as informações.

A *Cloud Act* vem como uma resposta para adequar a lei norte-americana às exigências da Convenção sobre Cibercrime (Convenção de Budapeste), para que os países que dela fazem parte tenham autoridade legal para obrigar empresas localizadas em seu território a divulgar dados, desde que respeitado o devido processo legal, mesmo que a empresa guarde os dados em outros países (ROSA; VIEIRA, 2019). Com as novas regras, o tempo de acesso às informações se tornou menor, pois antes, mesmo com os MLATs, alguns governos poderiam demorar bastante para enviar dados para outras nações.

6.5. Outros dispositivos legais dos EUA

Há, pelo menos, três outros dispositivos na legislação norte-americana que compõem o arcabouço legal para que as autoridades dos EUA possam acessar dados de terceiros. A Lei de Comunicações Armazenadas (SCA), a Lei de Privacidade das Comunicações Eletrônicas (ECPA) e a Lei de Compartilhamento de Informações de Segurança Cibernética (CISA).

A SCA – *Stored Communications Act* é uma lei de 1986, alterada pela Cloud Act, em 2018, para exigir que empresas dos EUA forneçam dados a agências governamentais independentemente de onde os dados estejam armazenados. A SCA permite o acesso a e-mails e a outras comunicações digitais, estabelecendo regras para a conduta para os agentes (CORNELL LAW SCHOOL, [s.d.]).

A ECPA – *Electronic Communications Privacy Act*, também de 1986, atualiza a lei federal sobre grampos telefônicos, de 1968. Inicialmente, a lei focava na interceptação de conversas usando linhas telefônicas analógicas. Porém, após o Patriot Act, tornou-se possível utilizá-la para o acesso às novas tecnologias de comunicação, o que inclui armazenamento de dados.

A CISA – *Cybersecurity Information Sharing Act* é uma lei que permite a colaboração e o compartilhamento de dados entre entidades federais autorizadas, como os departamentos de Comércio, Defesa, Energia, Justiça, Tesouro, Segurança Interna e o Gabinete do Diretor de Inteligência Nacional. A lei também foi criada para

proteger informações que estão armazenadas, em processamento ou em trânsito contra ameaças, vulnerabilidades ou problemas de cibersegurança.

Em síntese, o aparato legal norte-americano oferece ferramentas jurídicas inequívocas para vigilância eletrônica, coleta de dados e metadados em escala, capacidade de coerção das empresas privadas para que colaborem com as agências de governo dos EUA e para que alterem projetos para que grampos e violações sejam permitidas contra qualquer cliente.

6.6. Quadro-resumo

Tabela 6 – Quadro-resumo das Leis dos EUA

DISPOSITIVOS LEGAIS DOS ESTADOS UNIDOS DA AMÉRICA		
1	**FISA**	• Vigilância eletrônica; • Sem necessidade de autorização judicial para estrangeiros; • Governo dos EUA pode compelir empresas a colaborar; • Coleta de dados e de metadados.
2	**CALEA**	• Monitoramento de Voz sobre IP; • Monitoramento de tráfego via banda larga; • Fabricantes devem modificar projetos para permitir backdoors; • Operadoras devem informar Governo dos EUA em planos de segurança atualizados periodicamente; • Auxílio de provedores a autoridades policiais; • Assistência técnica para ajudar o Governo em interceptações; • Entrega de dados em formatos legíveis pelo Governo; • Operadoras devem mudar seus serviços para cumprirem a lei, se necessário.
3	**Patriot Act e Freedom Act**	• Uso da lei para combater crimes comuns e não somente terrorismo; • Grampos telefônicos; • Vigilância de comunicação eletrônica; • Equiparação da vigilância física com vigilância eletrônica; • Compartilhamento de informações entre agências de segurança e inteligência; • Possibilidade de alvos de espionagem ser investigados sem aviso prévio.
4	**Cloud Act**	• Provedor de serviços deve fazer backups de conteúdos dos clientes; • Divulgar registros ao Governos dos EUA, independentemente de onde foram capturados; • Palavra final será sempre da Justiça dos EUA; • Obtenção de dados com mais velocidade do que por meio de tratados bilaterais.
5	**SCA**	• Acesso a dados armazenados em qualquer país; • Violação de e-mails e comunicações digitais; • Empresas obrigadas a colaborar com o Governo dos EUA.
6	**ECPA**	• Atualização da lei de grampos para as novas tecnologias.
7	**CISA**	• Permite a colaboração e o compartilhamento de dados entre entidades federais autorizadas do Governo dos EUA.

Fonte: Elaborado pelo autor (CASSINO, 2025)

CAPÍTULO 7
PROPOSIÇÕES PARA FORTALECER A SOBERANIA DIGITAL

Qual a solução para a perda da soberania digital e da soberania de dados? Não é uma resposta fácil. Os Estados Unidos têm suas empresas de Tecnologia da Informação como pilares estratégicos de controle econômico, político, social, cultural e militar, como vimos nos capítulos anteriores. A República Popular da China, com suas próprias características, desenvolve tecnologias similares, que a colocam em uma relativa posição de autonomia frente aos EUA.

Os demais países acabam, em maior ou menor medida, sendo consumidores de tecnologias. As nações que integram a União Europeia têm mostrado desconforto com a situação, sobretudo após janeiro de 2025, quando Donald Trump assumiu a presidência dos EUA pela segunda vez, aproximou-se da Rússia, ameaçou sair da OTAN e declarou intenção de tomar a Groenlândia, que é um território da Dinamarca.

Cédric Durand (2025), no artigo *O tecnofeudalismo é um Leviatã frágil*, afirma que *"para escapar do processo de colonização digital, sua agenda deve ser a de uma política digital não alinhada com o objetivo de criar um espaço econômico para que as diferentes camadas constitutivas alternativas às Big Tech possam se desenvolver"*. É preciso impedir o terreno favorável às grandes corporações norte-americanas. Isso se daria de duas formas simultâneas: 1. uma nova forma de protecionismo digital; e 2. um internacionalismo tecnológico baseado na cooperação para operações em grandes escalas.

Durand defende que a resistência deve ter uma dimensão popular, com conscientização, envolvendo as massas nos debates políticos e tecnológicos, o que envolve discussões sobre o uso de ferramentas digitais. Deve-se criar uma tensão democrática que adicione contrapoderes às *Big Techs* e que estabeleça formas de controle, legitimando ações públicas, que, por sua vez, devem produzir políticas industriais e orientar investimentos.

Michael Kwet (2018) propõe um ecossistema digital que respeite a liberdade, que crie uma *"tecnologia do povo para o poder popular"* (*"People's Technology for*

People's Power"), que discuta modelos de propriedade e controle de infraestrutura sobre *software*, *hardware* e Internet. Os pilares para esse propósito seriam:

Primeiro, o fortalecimento do movimento internacional de *software* livre, cujas ideias de colaboração devem ser estendidas à produção de *hardwares* livres e a uma Internet com neutralidade de rede.

Em segundo lugar, a nuvem deve ser descentralizada, enfrentando o modelo de concentração em grandes corporações. O modelo atualmente dominante de computação em nuvem não é a única solução possível. Há alternativas, como o FreedomBox, um *software* livre, inspirado nas práticas de compartilhamento *peer-to-peer*, que pode ser instalado na máquina de cada usuário e que passa a colaborar com uma infraestrutura distribuída, sem intermediários centralizadores. Evidentemente, o modelo do FreedomBox apresenta limitações, mas ele demonstra que o modelo de nuvem corporativa em mega *data centers* não é o único possível.

O terceiro ponto é enfrentar a dominação ideológica da hegemonia tecnológica, combatendo as verdades impostas pelas empresas quando elas vendem seus pacotes de produtos como as únicas e melhores soluções disponíveis. Kwet acredita que é possível criar tecnologias para facilitar a educação, o compartilhamento, o controle sobre a propriedade, a democracia direta, a soberania local e a privacidade real.

7.1. Europa contra as *Big Techs*

Um artigo de Tulio Chiarini e Diandra Rocha (2024), para o portal do Instituto de Pesquisa Econômica Aplicada (IPEA), faz um bom resumo sobre como a União Europeia tem buscado enfrentar seus desafios no cenário tecnológico mundial, em especial quanto à marginalização das suas empresas frente às *Big Techs* norte-americanas e chinesas. Os desafios estariam divididos em criar um ambiente digital mais seguro, preservar direitos fundamentais, melhorar a competitividade no mercado de dados pessoais, reforçar a governança, incentivar a inovação e consolidar a soberania digital.

A partir de 2016, a União Europeia começou a aprovar novas leis para tentar melhorar sua posição estratégica no mundo digital. Primeiro, sancionou o

Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR) e começou a implementá-lo em 2018. O GDPR inspirou fortemente a Lei Geral de Proteção de Dados Pessoais do Brasil.

Em 2022, foram aprovadas a Lei de Serviços Digitais (*Digital Services Act* – DSA) e a Lei do Mercado Digital (*Digital Markets Act* – DMA). O DSA, aplicável após fevereiro de 2024, procura garantir a proteção dos usuários no mundo *online* ao exigir transparência das plataformas digitais. O DSA exige também que plataformas com número médio mensal de usuários ativos superior a 45 milhões estejam sujeitas a auditorias para avaliar o cumprimento da lei.

Na lista da DSA, datada de março de 2024, há 19 empresas, sendo 15 norte-americanas (das quais 11 são controladas pela GAFAM – Google/Alphabet, Apple, Facebook/Meta, Amazon e Microsoft), duas chinesas (Alibaba e TikTok), uma alemã (Zalando) e uma holandesa (booking.com).

Tabela 7 – Plataformas gigantes conforme a DSA europeia

Quadro 1 - Plataformas digitais muito grandes conforme definidas pela DSA

Plataformas digitais	Empresas controladoras	Países sedes
Alibaba AliExpress	Alibaba Group Holding Ltd.	China
Amazon Store	Amazon.com Inc.	EUA
AppStore	Apple Inc.	EUA
Booking.com	Booking Holdings	Holanda
Facebook	Meta Platforms Inc.	EUA
Google Play	Alphabet Inc.	EUA
Google Maps	Alphabet Inc.	EUA
Google Shopping	Alphabet Inc.	EUA
Instagram	Meta Platforms Inc.	EUA
LinkedIn	Microsoft Corp.	EUA
Pinterest	Pinterest Inc.	EUA
Snapchat	Snap Inc.	EUA
TikTok	ByteDance Ltd.	China
Twitter	X Holdings Corp.	EUA
Wikipedia	Wikipedia Foundation Inc.	EUA
YouTube	Alphabet Inc.	EUA
Zalando	Zalando SE	Alemanha
Bing	Microsoft Corp.	EUA
Google Search	Alphabet Inc.	EUA

Fonte: European Commission. Elaborado pelos autores

Fonte: European Comission. Elaboração: CHIARINI; ROCHA, 2024

A Lei do Mercado Digital (DMA), que começou a valer em 2023, é mais focada na concorrência dos mercados digitais e em impedir abusos de *Big Techs* dominantes. A lei denomina as grandes plataformas digitais como *“gatekeepers”* e impõe obrigações especiais a elas, como garantir interoperabilidade, acesso a dados e promoção de produção sem aprisioná-los em uma única plataforma. Práticas consideradas desleais ficam proibidas.

São consideradas *"gatekeepers"* as empresas que, dentre outros critérios, tenham faturamento anual mínimo de 7,5 bilhões de euros ou uma capitalização de mercado de 75 bilhões de euros, além de terem pelo menos 45 milhões de usuários ativos mensalmente na UE.

Em 2023, a União Europeia aprovou o Regulamento de Dados (*Data Act*) e o Regulamento da Inteligência Artificial (*AI Act*), que entrarão em vigor em 2025. Segundo o *site* EU Data Act (www.eu-data-act.com), essa lei estabelece regras sobre quem pode usar e quem pode acessar dados e para quais propósitos, em todos os setores econômicos.

Já o AI ACT, segundo o *site* oficial (www.artificialintelligenceact.eu), pode ser resumido em quatro pontos principais: 1. Sistemas de IA são classificados pelo risco que representam; 2. A maior parte das obrigações de IA de alto risco fica a cargo dos desenvolvedores dos sistemas; 3. Define que, para os termos da lei, usuários são pessoas físicas ou jurídicas que implantam um sistema de IA em caráter profissional, não usuários finais afetados; e 4. Aborda como deve ser feita a documentação da Inteligência Artificial, principalmente para IA de propósito geral.

7.2. A Iniciativa EuroStack

A iniciativa EuroStack é uma proposta de política industrial europeia para tecnologia, governança e financiamento para se construir infraestruturas digitais de conectividade, computação em nuvem, Inteligência Artificial e plataformas digitais, dentre outros setores. O projeto prevê a sustentação do empreendedorismo e da competitividade na Europa por meio de um diverso ecossistema de negócios. São objetivos declarados que a iniciativa proteja a autonomia e a soberania dos países envolvidos em um cenário mundial “volátil” e empodere pessoas e empresas

europeias. A EuroStack dispõe de um portal onde o projeto é explicado em detalhes (https://euro-stack.eu).

O projeto propõe articular recursos existentes de maneira federada, coordenando investimentos públicos e privados. Para tanto, os líderes da iniciativa trabalham para que o Parlamento Europeu e a Comissão Europeia abracem a ideia e ajudem a torná-la uma realidade.

Mais de uma centena de empresas assinaram uma carta aberta (EUROSTACK, 2025) pedindo comprometimento das autoridades europeias com a Iniciativa EuroStack. A carta estabelece objetivos imediatos, como criação de demanda para a indústria europeia e o compromisso do poder público do bloco europeu exercer seu poder de compra para adquirir soluções produzidas no continente. A ideia não seria excluir não-europeus, mas criar condições de competições *"mais justas"*, segundo opinião dos signatários.

O segundo ponto é criar *"agrupamentos"* e *"federações"*, com padrões comuns para a indústria, para que se possa fornecer alternativas europeias em escala. Deve-se criar uma estreita coordenação para reunir e alavancar ativos que hoje estão dispersos e que poderiam trabalhar em rede. Um exemplo são as soluções de *software* de código aberto e o estabelecimento de padrões de interoperabilidade, facilitando processos de integração. A prioridade dessa coordenação deve ser os recursos que atendam às necessidades de infraestrutura, com autonomia de *hardware*, de nuvem e de plataformas soberanas.

O terceiro ponto da carta aberta é priorizar serviços que tenham perspectivas reais de adoção, atendendo a necessidades concretas. Deve-se evitar gastar recursos com coisas que não serão utilizadas. Quem receber financiamentos deve contribuir com os ativos e ter disposição para compartilhá-los no modelo federado.

O quarto ponto para o EuroStack é desenvolver requisitos harmonizados, como certificações, para que usuários de nuvem pública/privada escolham serviços de nuvem soberana europeia para seus dados sensíveis. Esses serviços devem ser capazes de suportar interrupções decorrentes de leis extraterritoriais à União Europeia. Padrões de segurança cibernética europeia (EUCS)[20] também precisam ser elevados em termos de exigência e eficiência.

20 European Cloud Services Cybersecurity Certification Scheme (EUCS)

Os últimos dois pontos da carta referem-se a financiamento. O quinto ponto é revisar e redirecionar os planos existentes, priorizando projetos tangíveis, relevantes para o mercado e orientados a resultados. O sexto é criar um fundo de infraestrutura soberana para apoiar investimentos públicos.

7.3. Soberania e digitalização democrática na Europa

Simona Levi escreveu uma proposta para a soberania e a digitalização democrática da Europa, publicada como um *reflection paper* pelo Parlamento Europeu, em 2021. O ponto central da autora é que a base da digitalização deva ser os direitos humanos, além de outros valores europeus, como soberania de dados e conteúdo, justiça e empreendedorismo para todos. No entanto, nos dias atuais, serviços comuns como acesso à Internet, criação de conteúdo e armazenamento, comunicação interpessoal *online* e navegação na *web* estão sob controle das *Big Techs* não europeias.

Levi propõe um olhar para uma digitalização inclusiva, que envolva atores menores, pequenas e médias empresas, e cada cidadão, colocando-os como corresponsáveis pelo desenvolvimento de uma arquitetura digital democrática. Deve-se encarar como direitos elementos como o acesso à Internet para todos, privacidade e proteção de dados pessoais, inviolabilidade da comunicação e autodeterminação informacional (LEVI, 2021).

Os planos para uma transição digital europeia, para Levi, devem garantir ferramentas e infraestruturas que atendam ao dia a dia da população. Ela propõe três *"ações/protótipos"*, que são: 1. ferramentas operacionais e armazenamento para atividades cotidianas; 2. e-mail e comunicação interpessoal; 3. navegação na Internet. Essas soluções devem estar sob controle europeu, enfrentando as empresas que dominam o mercado. Mas as novas soluções precisam ser auditáveis de forma a garantir a soberania e a digitalização democrática.

7.4. Comuns digitais e a Infraestrutura Digital Pública Europeia

Schoemaker (2024), em artigo publicado no site do EuroStack, considera que uma Infraestrutura Digital Pública é o caminho que emerge para a transformação digital do poder público. Segundo o autor, esse tipo de infraestrutura pode ser definido como um conjunto de sistemas digitais compartilhados, seguros e interoperáveis, que sejam construídos com base em especificações e padrões abertos para entregar acesso equitativo a serviços públicos e/ou privados. Devem poder ser aplicados em escala que atenda ao conjunto da sociedade. E precisa ter um modelo de governança que incentive desenvolvimento, inclusão, inovação, confiança e respeito aos direitos humanos e às liberdades fundamentais.

Um dos fatores que podem oferecer uma oportunidade estratégica de longo prazo para a Europa, na opinião de Schoemaker, é que essas Infraestruturas Digitais Públicas sejam baseadas em “Comuns do Digital” (*Digital Commons*). A palavra *“Commons”* remete aos *“bens comuns”*, coisas cuja propriedade não pertence a ninguém e a todos ao mesmo tempo. Não é um bem privado nem um bem estatal, mas que pertence a toda comunidade. Elinor Ostrom (1990), ganhadora do Prêmio Nobel de Economia, mostrou como a gestão coletiva dos bens comuns (físicos) pode trazer excelentes resultados para uma comunidade.

Krewer e Warso (2024, p. 4) definem *Digital Commons* como tendo três características: 1. são um recurso digital (compostos por bits ou dígitos binários); 2. têm uma comunidade de produção distribuída e gestão coletiva; e 3. são definidos por um sistema de governança com regras estabelecidas para acesso e compartilhamento do recurso. Esses autores sugerem, então, que os *Digital Commons* sejam aplicados a uma Infraestrutura Digital Pública europeia. Eles argumentam que os Comuns Digitais podem ser uma possibilidade radical de um mundo além do mercado e do Estado, como uma terceira via para organizar a sociedade (Ibid., 2024, p. 37).

João Francisco Cassino (2019) mostrou, em sua dissertação de mestrado, como a política de implementação de *software* livre do Governo Federal do Brasil, entre 2003 e 2016, é um estudo de caso de uso de comuns do conhecimento na administração pública de um país do Sul global.

7.5. Propostas para o Brasil

André Lemos (2023, p. 36), em palestra no *Seminário Tecnologia no Brasil 2020-2030*, propôs dez pontos do que a sociedade brasileira deve fazer no futuro próximo no ambiente digital.

Para o professor, o primeiro ponto é avançar com a regulação, mas de uma forma que combine a regulação estatal com a autorregulação, criando uma corregulação, que envolva quadros jurídicos, tecnológicos e educacionais.

O segundo ponto é frear processos que ampliem formas de vigilância e discriminação, em especial a discriminação algorítmica. Em terceiro lugar, é preciso parar os abusos no uso de biometria, como reconhecimento facial por câmeras de vigilância em ambientes públicos.

O quarto ponto é a discussão sobre agência, o que Colin Koopman chama de *Infopower*. Esse conceito tenta explicar como a *"formatação"* de dados também *"formata"* o cidadão. Exemplo: se em um formulário houver apenas duas opções de gênero, homem e mulher, ao escolher um deles, a pessoa passa a estar categorizada daquela forma, excluindo opções alternativas. Esses dados serão processados por algoritmos e gerarão decorrências para a vida daquela pessoa. Os dados vão produzir o cidadão.

O quinto ponto é auditoria algorítmica para sistemas de relevância pública. O sexto ponto concerne à ampliação das diferenças e da pluralidade na representatividade (gênero, raça, classes sociais) na produção dos algoritmos.

O sétimo ponto é defender conquistas legislativas que já obtivemos, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, que sofrem ameaças constantes.

O oitavo ponto são os direitos trabalhistas nesta economia de plataformas (Uber, 99, iFood, etc.). O nono ponto é a formação e educação em computação e em humanidades digitais. O décimo ponto é a sustentabilidade ambiental, incluindo a pegada de carbono gerada pelos *data centers*, para que a Internet funcione.

7.6. Novas leis para o Brasil

Não é objetivo desta tese entrar no debate de projetos de lei que tramitam no Congresso Nacional brasileiro. No entanto, no momento em que ela é escrita, estão em andamento dois projetos legislativos que são de extrema importância para a evolução democrática do cenário digital no Brasil. São eles o PL 2338/2023, que trata do tema Inteligência Artificial, e o PL 2630/2020, também conhecido por Lei das *Fake News*.

O PL sobre Inteligência Artificial se propõe a regular o desenvolvimento, o fomento e o uso ético e responsável da IA no Brasil com base na centralidade da pessoa humana. Dois pontos importantes do projeto são uma abordagem de IA baseada em direitos e o estabelecimento de uma classificação de riscos.

O PL das *Fake News* busca criar normas de transparência para redes sociais e serviços de mensagens privadas (como WhatsApp), inclusive responsabilizando os provedores dos serviços pelo combate à desinformação. Também é objeto da lei a transparência em relação a conteúdos patrocinados, a forma de atuação do poder público e também as sanções para quem descumprir os termos legais.

Como os textos legais ainda não foram aprovados e sancionados, obviamente não estão em vigor. No entanto, mesmo que o conteúdo das propostas não tenha o rigor desejado por alguns políticos, militantes partidários, ativistas e outros membros de movimentos sociais do campo democrático e popular, os projetos podem representar avanços no cenário regulatório brasileiro.

7.7. Propostas para cidades

O Laboratório de Tecnologias Livres (LabLivre) da Universidade Federal do ABC (UFABC) publicou o *Guia Rápido sobre Soberania Digital e Soberania de Dados para Gestores Públicos Municipais do Brasil*, em 2024. É um pequeno manual de sugestões para prefeitos, vereadores e administradores públicos de nível municipal sobre o que eles poderiam fazer para reduzir a dependência das cidades em relação às *Big Techs* e outros grandes fornecedores de TI. O guia foi escrito de maneira didática e reforça pontos que os gestores devem observar.

O primeiro ponto é trabalhar com *“soberania digital e direitos by design”*, o que significa trabalhar com a ideia de soberania desde o momento de concepção de um novo projeto até o momento em que ele entra em produção para atender a população. A soberania deve estar na mente do gestor, do planejamento ao término da execução.

O segundo ponto é adotar ferramentas de *software* livre e/ou de código aberto. São produtos geralmente sem custos de licença de uso, que permitem maior controle e autonomia sobre as decisões tecnológicas do município, assim como garantem facilidade para auditorias e personalização.

O terceiro ponto é evitar a “distopia neoliberal” das cidades inteligentes (*smart cities*), que espalha sensores e câmeras de todos os tipos por todos os cantos das cidades e dentro dos prédios públicos, afetando a privacidade dos cidadãos e, nem sempre, trazendo resultados práticos para além de lucros para as corporações.

O quarto e o quinto pontos referem-se à participação cidadã no processo de decisão sobre quais tecnologias serão adotadas pela Prefeitura, sendo a criação de *“comitês de agentes digitais e de inteligência artificial para cidades inclusivas”* e a *“participação de técnicos e trabalhadores”* nas fases de deliberação dos projetos (LABLIVRE, 2024, p. 6-7).

O sexto ponto é que, quando a prefeitura for adotar ferramentas de IA, deve estar atenta a possíveis vieses dos sistemas algorítmicos. Sistemas digitais podem ser racistas, homofóbicos, misóginos ou reproduzir qualquer outro tipo de preconceito. Isso ocorre porque os sistemas são alimentados por dados humanos, produzidos por pessoas cujas atividades alimentam os bancos de dados, que acabam sendo impregnados por valores tanto positivos quanto negativos. Por fim, o guia recomenda que os gestores municipais façam uma boa análise de riscos, adotem transparência nos sistemas e os instalem em infraestruturas soberanas.

Os municípios brasileiros podem também aprender com experiências de outras cidades. Artigo de Francesca Bria (2020) relata a experiência de Barcelona, Espanha, no que ela chama de luta pela soberania digital. Um dos pontos centrais é tornar públicos os dados controlados por plataformas como Google, Uber e Airbnb. Essas informações, em vez de ficarem restritas às plataformas com o objetivo único

de gerarem lucros, devem ser utilizadas para melhorar serviços públicos, como os transportes, a saúde, a educação e a segurança.

Outra preocupação é com a dependência da cidade em relação ao poder da indústria tecnológica. Bria propõe repolitizar o debate sobre o uso dessas tecnologias, com foco na distribuição dos bens e do poder, assim como na gestão pública e nas infraestruturas críticas. As cidades, por serem menores, podem ser laboratórios para exercitar o uso de dados e de algoritmos com uma lógica de solidariedade, cooperação social e direitos coletivos.

A recuperação da soberania digital na cidade passa por criar mecanismos de participação cidadã nas decisões sobre o funcionamento das infraestruturas tecnológicas. Isso faria parte de uma agenda política e econômica mais ampla para recuperar as cidades impactadas pela *"virada neoliberal"* na política urbana, segundo a autora.

Como intervenções práticas, para Bria, podem ser listadas a exigência de soluções de *software* livre e de código aberto nos projetos de cidades inteligentes, a inclusão de cláusulas sobre soberania de dados nos contratos e a definição de padrões éticos para o processo de digitalização, que devem ser obrigatórios ao funcionalismo público. Por fim, os dados gerados nas cidades e capturados pelos sistemas de informação precisam ter seu valor econômico devolvido aos cidadãos, como com a criação de bases de dados como um bem comum.

CONCLUSÃO

A hipótese desta tese de doutorado era que *"as soluções tecnológicas que o Estado brasileiro está adotando para superar as condições de perda de soberania digital e de soberania de dados são insuficientes. Os produtos e serviços dos modelos de 'nuvens soberanas' em implantação tornam o Estado refém de fornecedores estrangeiros e vulnerável à perda de dados"*.

Apresentou-se como o ecossistema de infraestruturas do digital está dividido em camadas, sendo que, em todas elas, há dificuldades de gestão soberana pelo Brasil. Foi feita a análise de leis, de normas e de práticas do Estado brasileiro, em especial da estatal Serpro. Observou-se as regras de contratos e licenças com os principais fornecedores de nuvem. Avaliamos dispositivos da legislação norte-americana que obrigam suas empresas a criar mecanismos de vigilância em *hardwares* e *softwares* necessários ao funcionamento do ambiente digital.

Acredito estar provado que os dispositivos legais e as formas técnicas de funcionamento das tecnologias digitais eliminam qualquer possibilidade de argumentação de que o Brasil está construindo uma soberania digital. Pelo contrário, a adoção das tecnologias de nuvem estrangeira está piorando a situação. Quando o Serpro mantinha os sistemas do Estado em *data center* próprio e utilizava preferencialmente *softwares* livres, havia mais soberania.

Adotar a estratégia de se criar uma 'Nuvem de Governo' para guardar as informações sensíveis em parceria com as *Big Techs* norte-americanas é um retrocesso, pois aumenta o poder das empresas sediadas nos Estados Unidos de violarem a soberania digital brasileira caso necessitem.

Como demonstrado, as leis dos EUA obrigam as empresas a fornecerem informações. A CALEA é uma lei que exige que os fabricantes de *hardware* instalem *backdoors* em seus equipamentos.

Para tratarmos de *soberania digital*, não basta olhar apenas um elemento isolado. Precisamos observar todo o ecossistema envolvido e debater a capacidade de controle estatal de maneira geral. O Brasil tem uma situação privilegiada quanto ao potencial de geração de energia elétrica, mas tem perdido autonomia nos últimos anos com a privatização progressiva do sistema elétrico. O setor de

telecomunicações, também privatizado, caminha para a universalização da conectividade, mas com níveis de qualidade muito diferentes a depender da localização geográfica e da capacidade econômica do público pagante. Quanto aos *data centers*, o Brasil vem liderando a instalação deste tipo de infraestrutura na América Latina, mas os números ainda são extremamente pequenos para o tamanho e potencial do país, além de serem muito concentrados na região Sudeste. A fabricação de *hardwares* e equipamentos até conta com um número razoável de empresas, cerca de 3 mil, mas que estão longe da fronteira tecnológica, atuando mais como montadoras de itens importados. Com a criação da Ceitec, o Brasil tentou ingressar como ator internacional para a produção de semicondutores, mas a empresa, além de dificuldades típicas de sua atividade econômica, foi alvo de uma tentativa de liquidação durante o Governo Bolsonaro.

Sobre uso e desenvolvimento de *softwares* básicos, o Brasil, que foi referência global em *software* livre no início dos anos 2000, abandonou completamente essa política e também sofre com escassez de mão de obra especializada. Já o desenvolvimento de sistemas e aplicativos é baseado em empresas privadas e em *startups*, cuja capacidade de exportação de *software* é irrisória, mesmo o Brasil sendo o 10º maior mercado de TICs do mundo. As gigantescas e riquíssimas bases de dados do Estado brasileiro, ainda que parcialmente protegidas pela Lei Geral de Proteção de Dados Pessoais, são alvo da cobiça das empresas de tecnologia, ávidas por dados para alimentar seus sistemas de *Big Data* e de Inteligência Artificial. Sobre IA, o país se esforça para investir como ator global, mas o montante é apenas um fragmento do que fazem EUA e China.

O Brasil precisa observar melhor o que tem feito a União Europeia, ao investir para tentar, ao menos em princípio, criar infraestruturas soberanas, com interoperabilidade, *softwares* livres e de código aberto, comuns digitais e compromisso estatal em garantir maior autonomia.

REFERÊNCIAS BIBLIOGRÁFICAS

a) Bibliografia Acadêmica

AVELINO, Rodolfo da Silva. **Tecnologias de Rastreamento Online e a Economia Informacional.** Tese de Doutorado. São Bernardo do Campo-SP. UFABC, 2021.

BELLI, Luca. ***Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, towards an AI Sovereignty Stack*.** In: Carnegie Endowment for International Peace. *Digital Democracy Network Conference 2023 Essay Collection*. [S.l.], 2023.

BODIN, Jean. **Os Seis Livros da República.** Publicação original: 1576. Tradução de Tarcísio Pimenta. 1ª ed. Brasília: Editora UnB, 1997.

BRATTON, Benjamin H. **The Stack | On Software and Sovereignty.** The MIT Press. Cambridge, Massachusetts. London, England, 2015.

BRIA, Francesca. **Public policies for digital sovereignty.** In: T. Scholz, N. Schneider (eds.), Ours to Hack and to Own: The Rise of Platform Cooperativism, A New Vision for the Future of Work and a Fairer Internet. (1ª ed. p. 218-222). N.York/London: OR Books, 2017.

_____. **Barcelona propõe a luta pela soberania digital**. O Partisano, 30 nov. 2020. Disponível em: <https://outraspalavras.net/outrasmidias/barcelona-propoe-a-luta-pela-soberania-digital>. Acesso em: 22 abr. 2025.

_____. **Putting tech and innovation at the service of people and the green transition.** Em: 9 mar 2020. In: UCL Institute for Innovation and Public Purpose, 2020. Disponível em: https://medium.com/iipp-blog/putting-tech-and-innovation-at-the-service-of-people-and-the-green-transition-2e039ab8e083. Acesso em: 8 abr 2025.

CASSINO, João Francisco. **Implementação de software livre no governo federal: um estudo de caso de adoção do comum**. Universidade Federal do ABC. Programa de Pós-Graduação em Ciências Humanas e Sociais. São Bernardo do Campo – SP, 2019. Disponível em: <https://biblioteca.ufabc.edu.br/mobile/download.php?idioma=ptbr&acesso=web&codigo=80008&tipo_midia=2&iUsuario=0&obra=122547&tipo=1&downloadApp=1>. Acesso em: 12 abr. 2025.

CASSINO, João Francisco; SILVEIRA, Sérgio Amadeu da. SOUZA, Joyce (Orgs.). **Colonialismo de Dados: Como Opera a Trincheira Algorítmica na Guerra Neoliberal.** Editora Autonomia Literária. São Paulo-SP, 2021.

CERVO, Amado Luiz. **Hegemonia coletiva e equilíbrio: a construção do mundo liberal (1815-1871).** In: História das Relações Internacionais Contemporâneas - da sociedade internacional do século XIX à era da globalização. 2ª edição revista e atualizada. SARAIVA, José Flávio Sombra (Org.). São Paulo: Saraiva, 2007.

CHIARINI, Tulio; ROCHA, Diandra. **União Europeia contra as big techs - Regulações digitais para equidade e segurança.** Centro de Pesquisa em Ciência, Tecnologia e Sociedade (CTS) do Ipea, 13 mar. 2024. Disponível em: <https://www.ipea.gov.br/cts/en/topics/417-uniao-europeia-contra-big-techs>. Acesso em: 22 abr. 2025.

COULDRY, Nick; MEJIAS, Ulises A. **The Costs of Connection - How Data Is Colonizing Human Life and Appropriating It for Capitalism.** Stanford University Press. Standord, Califórnia, 2019.

DURAND, Cédric. **Tecnofeudalismo: Crítica de la economía digital.** 1ª ed. - Adrogué: La Cebra/Donostia:Kaxilda, 2021a. 288p.

_____ . **A hipótese do Tecnofeudalismo**. [Entrevista para] IHU, 2021b. Disponível em: https://outraspalavras.net/outrasmidias/a-hipotese-dotecnofeudalismo . Acesso em 7 abr 2025.

_____ . **O tecnofeudalismo é um Leviatã frágil.** Instituto Humanitas Unisinos - IHU, 03 fev. 2025. Disponível em: <https://www.ihu.unisinos.br/categorias/648647-o-tecnofeudalismo-e-um-leviata-fragil-artigo-de-cedric-durand>. Acesso em: 22 abr. 2025.

FANON, Frantz. **Pele negra, máscaras brancas.** Publicação original: 1952. Edição atual: Ubu Editora, 2020.

_____ . **Os Condenados da Terra.** Publicação original: 1961. Edição atual: Ed. Zahar, 2021.

FARIAS, Regina Cláudia Gondim Bezerra. **Atuação Estatal e a Privatização do Setor Elétrico Brasileiro.** Universidade de Brasília – UNB, Instituto de Ciência Política – IPOL. Brasília, 2006.

FERNANDES, Irineu Barreto. **Contratualistas – Soberania**. Videoaula. IFTM - Campus Uberlândia, 2020. Disponível em: https://www.youtube.com/watch?v=oT5eodceKRE . Acesso em: 8 abr 2025.

GALIJ, Stanisław; PAWLAK, Grzegorz; GRZYB, Sławomir. **Modeling Data Sovereignty in Public Cloud—A Comparison of Existing Solutions**. 2024. Appl. Sci. 2024, 14(23), 10803; https://doi.org/10.3390/app142310803. Disponível em: https://www.mdpi.com/2076-3417/14/23/10803. Acesso em: 8 abr 2025.

GALLOWAY, Alexander R. **Protocol: How Control Exists after Decentralization.** Cambridge, Massachusetts; London, England: The MIT Press, 2004.

GLOBERMAN, S. **Canadian science policy and technological sovereignty.** 1978. Canadian Public Policy/Analyse De Politiques, 4(1), 34-45.

GRAY, Catriona. **More than Extraction: Rethinking Data's Colonial Political Economy.** In: International Political Sociology, Volume 17, Issue 2, June 2023. Disponível em: https://doi.org/10.1093/ips/olad007. Acesso em: 7 abr 2025.

HEEFNER, Gretchen. **“A Slice of their Sovereignty”: Negotiating the U.S. Empire of Bases, Wheelus Field, Libya, 1950-1954.** Diplomatic History Advance. Access published December 4, 2015. Disponível em: http://dh.oxfordjournals.org. Acesso em 8 abr 2025.

KWET, Michael. **Digital colonialism – The evolution of US empire.** In: TNI LongReads, 4 mar 2021. Disponível em: https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire. Acesso em 7 abr 2025.

_____ . **Digital Colonialism: US Empire and the New Imperialism in the Global South.** 15 ago 2018. Para versão final, ver: Race & Class Volume 60, No. 4 (April 2019); Disp. em: https://ssrn.com/abstract=3232297. Acesso em 7 abr 2025.

_____ . **Digital Degrowth: Technology in the Age of Survival.** Pluto Press, Londres, Inglaterra, 2024.

KREWER, Jan; WARSO, Zuzanna. **Digital Commons as Providers of Public Digital Infrastructure.** 13 Nov. 2024. Open Future. Disponível em: https://openfuture.eu/wp-content/uploads/2024/11/241113_Digital-Commons-as-Providers-of-Public-Digital-Infrastructures.pdf. Acesso em: 22 abr. 2025.

LABLIVRE - LABORATÓRIO DE TECNOLOGIAS LIVRES. **Guia rápido sobre soberania digital e soberania de dados para gestores públicos municipais do Brasil.** 2024. Universidade Federal do ABC (UFABC). Disponível em: https://lablivre.pesquisa.ufabc.edu.br/wp-content/uploads/2024/10/GUIA-SOBERANIA-DIGITAL-PARA-GESTORES-MUNICIPAIS.pdf. Acesso: 22 abr 2025.

LEMOS, André. **Plataformas digitais: o que incentivar, o que limitar e o que vetar.** Primeiro encontro. Parte 1 In: PENTEADO, Cláudio; PELLEGRINI, Jerônimo. SILVEIRA, Sérgio Amadeu da. Plataformização, Inteligência Artificial e Soberania de Dados. Tecnologia no Brasil 2020-2030. Ação Educativa, 2023.

LEVI, Simona. **Proposal for a Sovereign and Democratic Digitalisation of Europe Reflection Paper commissioned by David Sassoli to the team led by Simona Levi (Xnet).** Publications Office of the European Union (December 2021). Disponível em: https://op.europa.eu/en/publication-detail/-/publication/dae77969-7812-11ec-9136-01aa75ed71a1. Acesso em: 22 abr 2025.

_____. **Digitalización Democrática: Soberanía Digital para las Personas.** Rayo Verde Editorial, 2024.

MACEDO JÚNIOR, Ronaldo Porto. **Constituição, soberania e ditadura em Carl Schmitt**. Universidade de São Paulo (USP), 1997. In: Scielo. Disponível em: https://www.scielo.br/j/ln/a/Jhcwj5QQxR7HtYtVK5c7yBv. Acesso em 8 abr 2025.

MACIEL, Marília. In: **Seminário Internacional de Governança da Internet - Eixo 1 – Mesa 2: Os desafios da governança global da Internet e a construção de espaços multissetoriais,** 30 mar 2021, p. 6-17. Disponível em: https://cgi.br/media/pdf/egi/202104-Transcricao_Seminario_Internacional_Governanca_Internet_eixo1_mesa2.pdf. Acesso em: 8 abr 2025.

MAQUIAVEL, Nicolau. **O Príncipe.** Publicação original: 1532. Tradução de Lívio Xavier. 1ª ed. São Paulo: Editora Martin Claret, 2008.

MORAES, Gabriel Boscardim de. **As parcerias das big techs com o Estado brasileiro e a soberania digital: o caso do SERPRO.** Santo André: Universidade Federal do ABC, Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, 2024. Trabalho de conclusão de curso. Disponível em: https://bpp.ufabc.edu.br/site/wp-content/uploads/2024/10/TCC-Gabriel-Moraes.pdf. Acesso em: 20 abr 2025.

MOULIER-BOUTANG, Yann. **Le capitalisme cognitif: La nouvelle grande transformation.** Paris: Éditions Amsterdam, 2007a.

_____ . **A bioprodução. "O capitalismo cognitivo produz conhecimentos por meio de conhecimento e vida por meio de vida"**. [Entrevista para] IHU ONLINE. Revista do Instituto Humanitas Unisinos, Edição 216, em 23 de abril de 2007b. Disponível em: https://www.ihuonline.unisinos.br/artigo/858-yann-moulier-boutang-1. Acesso em 19 jan 2025.

MOROZOV, Evgeny. **Uma crítica da razão tecno-feudal.** New Left Review n. 133/134. In: Eleutério F S Prado. Publicado em 20 nov 2022. Disponível em: https://eleuterioprado.blog/2022/11/20/uma-critica-da-razao-tecno-feudal/ Acesso em 19 jan 2025.

OSTROM, Elinor. **Governing the Commons: The Evolution of Institutions for Collective Action**. 30 novembro 1990.

POLIDO, Fabrício Bertini Pasquot. **Estado, soberania digital e tecnologias emergentes interações entre direito internacional, segurança cibernética e inteligência artificial.** In: Revice - Revista de Ciências do Estado, v. 9 n. 1 (2024): Estado e soberania na era cibernética / Dossiê. Universidade Federal de Minas Gerais (UFMG). Disponível em: https://periodicos.ufmg.br/index.php/revice/article/view/e53066. Acesso em: 8 abr 2025.

ROSA, Sérgio. Entrevista concedida a SOUZA, Joyce Ariane de. **Tecnologias de Dataficação e o Aprofundamento do Neoliberalismo na Saúde Brasileira**. Tese de doutorado. Universidade Federal do ABC (UFABC), S. Bernardo do Campo, 2023.

SCHIAVI, Iara.; SILVEIRA, Sérgio Amadeu da. **A cidade neoliberal e a soberania de dados: mapeamento do cenário dos dispositivos de dataficação em São Paulo.** 2022. urbe. Revista Brasileira de Gestão Urbana, v.14, e20210145.

SCHILLER, Daniel. **Digital Capitalism: Networking the Global Market System**. MIT Press, 1999. Disponível em: **https://direct.mit.edu/books/book/2755/Digital-CapitalismNetworking-the-Global-Market** . Acesso em 19 jan 2025.

SCHOEMAKER, Emrys. **Digital Commons and the European DPI Agenda.** Caribou Digital, DCTF Member, out. 2024. Disponível em: <https://euro-stack.eu/digital-commons-and-the-european-dpi-agenda>. Acesso em: 22 abr. 2025.

SILVEIRA, Sérgio Amadeu da. **Capitalismo Digital.** Revista Ciências do Trabalho n. 20, Dieese, 2021. Disponível em: **https://rct.dieese.org.br/index.php/rct/article/view/286/pdf** . Acesso em 19 jan 2025.

_____. **A ideologia da transformação digital.** Automatismos, solucionismos e alienação técnica. Revista Linguagem em Foco, v.15, n.3, 2024. p. 11-25. Disponível em: https://revistas.uece.br/index.php/linguagememfoco/article/view/12380. Acesso em 7 abr 2025.

SOUZA, Joyce Ariane de. **Tecnologias de Dataficação e o Aprofundamento do Neoliberalismo na Saúde Brasileira**. Tese de doutorado. Universidade Federal do ABC (UFABC), São Bernardo do Campo-SP, 2023.

SRNICEK, Nick. **Platform Capitalism.** Cambridge: Polity Press, 2017. 171 p.

STRANGE, Susan. **States and Markets.** London: Pinter Publishers, 1988.

VAN DIJCK, José. **Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology.** Surveillance & Society 12(2): 197-208, 2014. University of Amsterdam, The Netherlands. Disponível em: http://www.surveillance-and-society.org . Acesso em 19 jan 2025.

VAROUFAKIS, Yanis. **Estamos fazendo a transição do capitalismo para a servidão tecnofeudalista?** In: portal Jacobina, 2024. Disponível em: https://jacobin.com.br/2024/02/estamos-fazendo-a-transicao-do-capitalismo-para-a-servidao-tecnofeudalista . Acesso em 19 jan 2025.

_____ . **O tecnofeudalismo está dominando.** In: portal Jacobina, 2023. Disponível em: https://jacobin.com.br/2023/11/o-tecno-feudalismo-esta-dominando . Acesso em 7 abr 2025.

VILLAVERDE, Adão. **Os semicondutores, o caminho para a superação da dependência tecnológica no setor e o papel da CEITEC.** 2023. Tese (Doutorado em Educação em Ciências) — Instituto de Ciências Básicas da Saúde, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023. Orientador: Prof. Dr. Livio Amaral.

ZUBOFF, Shoshana. **Big other: Surveillance Capitalism and the Prospects of an Information Civilization**. Sage Journals, 2015. Disponível em: https://journals.sagepub.com/doi/10.1057/jit.2015.5 . Acesso em 19 jan 2025.

_____ . ***The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.*** New York: Public Affairs, 2019.

b) Estudos, Fontes Primárias e Oficiais

ADVISIA. **Produto VII | Relatório II – Iniciativa estratégica n° 19: Promover a articulação e a cooperação para o desenvolvimento de novas tecnologias.** RELATÓRIO PARA A ITU E ANATEL. Contrato: S-BDT-2023-006. 23 abr 2023. Disponível em: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/c8b07fa359307f48e93cdfc12cd409f0. Acesso em: 10 abr 2025.

AGÊNCIA GOV. **Lula recoloca a Telebras no jogo: 'Não é preciso desmontar o Estado'**. 2024. Agência Gov, 27 ago. 2024. Disponível em: https://agenciagov.ebc.com.br/noticias/202408/lula-recoloca-a-telebras-no-jogo-nao-e-preciso-desmontar-o-estado. Acesso em: 10 abr. 2025.

AWS – AMAZON WEB SERVICES. **Amazon Web Services to launch AWS European Sovereign Cloud.** 10 out. 2023. Disponível em: <https://press.aboutamazon.com/2023/10/amazon-web-services-to-launch-aws-european-sovereign-cloud>. Acesso em: 18 abr. 2025.

_____. **Certification Exams.** 2024a. Disponível em: <https://aws.amazon.com/pt/certification/exams/>. Acesso em 19 abr 2025.

_____. **Global Infrastructure Regions and Availability Zones.** 2024b. Disponível em: <https://aws.amazon.com/pt/about-aws/global-infrastructure/regions_az/>. Acesso em: 20 abr. 2025.

_____. **Digital Sovereignty**. 2025. Disponível em: <https://aws.amazon.com/pt/compliance/digital-sovereignty/>. Acesso: 09 abr 2025.

_____. **Nuvem privada on premises - AWS Outposts**. [s.d]. Disp.: https://aws.amazon.com/pt/outposts. Acesso: 19 abr. 2025.

ABES – ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE. **Mercado Brasileiro de Software: panorama e tendências, 2023.** 1ª ed. São Paulo, 2024.

_____. **ABES anuncia novo presidente e nova diretoria com foco em inovação e soberania digital.** Publicado em: 25 mar 2025. Disponível em: https://abes.com.br/abes-anuncia-novo-presidente-e-nova-diretoria-com-foco-em-inovacao-e-soberania-digital-2/?utm_campaign=abes_informa_novo_presidente_da_abes_estudo_de_mercado_ciberseguranca_reforma_tributaria_noticias_de_associadas_e_muito_mais_-_31032025&utm_medium=email&utm_source=RD+Station. Acesso em: 18 abr 2025.

BANCO CENTRAL DO BRASIL. **OpenFinance.** [s.d]. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/openfinance>. Acesso em: 13 abr 2025.

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

_____. **Decreto nº 3.810, de 02 de maio de 2001.** Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=3810&ano=2001&ato=c1cUTSE90MNpWT07a>. Acesso em: 09 abr 2025.

_____**. Lei nº 13.303, de 30 de junho de 2016. Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm>. Acesso em: 18 abr. 2025.

_____. Instituto Nacional da Propriedade Industrial. **Modalidades de contratos e informações.** 31 jul 2017. Disp. em: <https://www.gov.br/inpi/pt-br/servicos/contratos-de-tecnologia-e-de-franquia/tipos-de-contratos>. Acesso em: 19 abr. 2025.

_____. Presidência da República. **Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação.** Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art6i. Acesso em 18 abr 2025.

_____. Supremo Tribunal Federal. **Medida Cautelar na Ação Declaratória de Constitucionalidade 51 Distrito Federal.** 10 mai 2019a. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15340132050&ext=.pdf>. Acesso em: 09 abr 2025.

_____, Ministério da Gestão e Inovação em Serviços Públicos. **Sobre o Catálogo de Bases de Dados.** Governo Digital. Publicado em: 28 nov. 2019b. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/sobre_catalogo-de-bases-de-dados. Acesso em: 13 abr 2025.

_____, Presidência da República. **Decreto nº 10.222, de 5 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 18 abr 2025.

_____, Gabinete de Segurança Institucional. **Instrução Normativa nº 5, de 30 de agosto de 2021.** Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684. Acesso em 18 abr 2025.

_____, ANATEL – Agência Nacional de Telecomunicações. **Infográfico Setorial de Telecomunicações.** Mar 2022a. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO47apD83dF28kmxvBGOSe3BkmePIJxRkSvu0TtBAAgHMGcDroTWLpVeS5GRal1Wc_Bo4dK9_oIywQeezXovdPNW. Acesso em: 10 abr 2025.

_____, Ministério da Ciência, Tecnologia e Inovação. **Estratégia Brasileira para a Transformação Digital (E-Digital). Ciclo 2022-2026.** Brasília, 2022b. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf. Acesso em: 18 abr 2025

_____, Presidência da República. **Decreto autoriza reversão do processo de liquidação e estabelece retomada operacional da Ceitec.** 06 nov. 2023a. Disponível em: <https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2023/11/decreto-autoriza-reversao-do-processo-de-liquidacao-e-estabelece-retomada-operacional-da-ceitec>. Acesso em: 10 abr. 2025.

_____, Agência Brasileira de Desenvolvimento Industrial (ABDI). **Estratégia para a implementação de política pública para atração de data centers.** Brasília, 2023b.

_____, Ministério da Defesa. **OFÍCIO nº 16-A4.7/A4/GabCmtEx.** Publicado em 6 jun 2024a. Disponível em: https://static.poder360.com.br/2024/08/Starlink-oficio-camara-jun2024.pdf. Acesso em: 8 abr 2025.

_____, Ministério da Gestão e da Inovação em Serviços Públicos. **Gestão assina acordos com Serpro e Dataprev para criação de Nuvem de Governo**. 12 nov 2024b. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2024/novembro/gestao-assina-acordos-com-serpro-e-dataprev-para-criacao-de-nuvem-de-governo>. Acesso em: 09 abr 2025.

_____, Governo Digital. **Estratégia Brasileira de Governo Digital 2024-2027.** Publicado em: 21 jun 2024c. Disponível em: https://www.gov.br/governodigital/pt-br/noticias/governo-federal-lanca-estrategia-nacional-de-governo-digital. Acesso em 13 abr 2025.

_____, Ministério da Ciência, Tecnologia e Inovação. **IA para o Bem de Todos. Proposta de Plano Brasileiro de Inteligência Artificial 2024-2028.** Reunião do Pleno do Conselho Nacional de Ciência e Tecnologia. 29 jul 2024d. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/07/plano-brasileiro-de-ia-tera-supercomputador-e-investimento-de-r-23-bilhoes-em-quatro-anos/ia_para_o_bem_de_todos.pdf/@@download/file. Acesso em: 13 abr 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. ***Gestão orienta órgãos sobre contratação e uso de serviços de computação em nuvem*.** Publicado em: 28 mar. 2024e. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2024/marco/gestao-orienta-orgaos-sobre-contratacao-e-uso-de-servicos-de-computacao-em-nuvem>. Acesso em: 19 abr. 2025.

_____. Controladoria-Geral da União. **Agência Nacional de Energia Elétrica - ANEEL**. Portal da Transparência. 2025a. Disp. em: <https://portaldatransparencia.gov.br/orgaos/32210-agencia-nacional-de-energia-eletrica>. Acesso: 10 abr. 2025.

_____, Ministério do Desenvolvimento, Indústria, Comércio e Serviços. **Nova Indústria Brasil - Plano de Ação 2024-2026.** 13 fev. 2025b. Disponível em: <https://www.gov.br/mdic/pt-br/composicao/se/cndi/plano-de-acao/nova-industria-brasil-plano-de-acao-2024-2026-1.pdf>. Acesso em: 10 abr. 2025.

_____, FINEP. **Comissão do Congresso aprova aumento de R$ 2 bilhões no orçamento do FNDCT para 2025.** 20 mar. 2025c. Disponível em: http://www.finep.gov.br/noticias/todas-noticias/6934-comissao-do-congresso-aprova-aumento-de-r-2-bilhoes-no-orcamento-do-fndct-para-2025. Acesso em: 13 abr. 2025.

_____, Governo Digital. **Nuvem de Governo.** 2025d. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/ambiente-tecnologico/nuvem/nuvem-de-governo. Acesso em 18 abr 2025.

_____. **Portaria COAF nº 4**, de 20 de março de 2025e. Diário Oficial da União. Disp. em: https://www.cnmp.mp.br/portal/images/Corregedoria/Recomendacoes/2025/Recomendacao-de-carater-geral-CN-n-4.25---versao-DOU-certificada.pdf. Acesso em: 20 abr 2025.

GCE S/A. **Data Center do Banco do Brasil e da Caixa Econômica Federal.** [s.d.] Disponível em: <https://www.gce.com.br/obra/1/11/data_center_do_banco_do_brasil_e_da_caixa_economica_federal>. Acesso em: 11 abr. 2025.

CGI.br. **Perto da universalização do acesso à internet, Brasil ainda tem maioria da população com baixa conectividade significativa, revela novo estudo.** 15 abr 2024. Conselho Gestor da Internet do Brasil. Disponível em: https://cgi.br/noticia/releases/perto-da-universalizacao-do-acesso-a-internet-brasil-ainda-tem-maioria-da-populacao-com-baixa-conectividade-significativa-revela-novo-estudo/. Acesso em: 10 abr. 2025.

CNI – CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. **Conheça a indústria brasileira de equipamentos de informática, produtos eletrônicos e ópticos**. 14 mar. 2022. Disponível em: <https://noticias.portaldaindustria.com.br/noticias/economia/conheca-a-industria-brasileira-de-equipamentos-de-informatica-produtos-eletronicos-e-opticos/>. Acesso em: 10 abr. 2025.

_____. **Importância da Indústria no Brasil.** 10 mar. 2025. Disponível em: <https://www.portaldaindustria.com.br/estatisticas/importancia-da-industria/>. Acesso em: 11 abr. 2025.

CAMELO, Ana Paula et al. **Soberania digital: para quê e para quem? Análise conceitual e política do conceito a partir do contexto brasileiro.** São Paulo: CEPI FGV DIREITO SP; ISOC Brasil, 2024. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/3f5fe812-9256-4c2c-8643-cd15a82c048e/content. Acesso: 18 abr 2025.

CARTA PÚBLICA CONTRA O ATAQUE DAS BIG TECHS À SOBERANIA DIGITAL, em 14 set 2024. Disp. em: https://capitaldigital.com.br/wp-content/uploads/2024/09/Brazil-Letter-fv_240914_PT.pdf. Acesso em: 8 abr 2025.

CORNELL LAW SCHOOL. **18 U.S. Code Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access. SCA.** [s.d.]. Disponível em: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>. Acesso em: 22 abr. 2025.

EMERGE. **Relatório Deep Techs Brasil 2024.** Disponível em: https://static.poder360.com.br/2024/11/Emerge-Relatorio-Deep-Techs-Brasil-2024-1.pdf. Acesso em: 12 abr 2025.

EUROSTACK. **EuroStack Initiative Letter**, 14 mar. 2025. Disponível em: <https://euro-stackletter.eu/wp-content/uploads/2025/03/EuroStack_Initiative_Letter_14-March-.pdf>. Acesso em: 9 abr. 2025.

FBI. **Foreign Intelligence Surveillance Act (FISA) and Section 702.** 1º dez 2023. Disponível em: <https://www.fbi.gov/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702>. Acesso em: 22 abr. 2025.

FCC NEWS. **FCC bans equipment authorizations for chinese telecommunications and video surveillance equipment deemed to pose a threat to national security.** Washington, USA, 25 nov 2022. Disp. em: https://docs.fcc.gov/public/attachments/DOC-389524A1.pdf. Acesso em: 8 abr 2025.

FLEMING, Sean. **What is digital sovereignty and how are countries approaching it?** Publicado em 10 jan 2025. Site do World Economic Forum. Disponível em: https://www.weforum.org/stories/2025/01/europe-digital-sovereignty. Acesso em: 8 abr 2025.

FLINDERS, Mesh; SMALLEY, Ian. **O que é soberania de dados?** Publicado em: 10 jun 2024. Site da IBM. Disponível em: https://www.ibm.com/br-pt/think/topics/data-sovereignty. Acesso em: 8 abr 2025.

GOOGLE. **Sovereign Cloud**. 2025. Disponível em: <https://cloud.google.com/sovereign-cloud?hl=pt-BR>. Acesso em: 09 abr 2025.

_____. **Google Distributed Clouds: Air-gapped approach to zero trust.** 17 jul 2024. Disponível em: <https://cloud.google.com/blog/products/identity-security/google-distributed-clouds-air-gapped-approach-to-zero-trust>. Acesso: 18 abr. 2025.

GOOGLE CLOUD. **Service Terms.** 21 out. 2024. Disponível em: <https://cloud.google.com/terms/gdcag/service-terms?hl=pt_br>. Acesso: 20 abr 2025.

GOOVAERTS, Diana. **‘There’s no escaping’ the rise of digital sovereignty, Google Cloud exec says.** Publicado em: 21 nov 2024. Site da Fierce Network. Disponível em: https://www.fierce-network.com/cloud/theres-no-escaping-rise-digital-sovereignty-google-cloud-exec-says. Acesso em: 8 abr 2025.

INTEL.GOV. **Categories of FISA.** [s.d.]. Disponível em: <https://www.intel.gov/foreign-intelligence-surveillance-act/1234-categories-of-fisa>. Acesso em: 22 abr. 2025.

LULA DA SILVA, Luiz Inácio. **Discurso do presidente Lula na abertura da 79ª Assembleia Geral da ONU**, em Nova Iorque, EUA. Em 24 set 2024. Transcrição. Disponível em: https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/discursos-e-pronunciamentos/2024/09/discurso-do-presidente-lula-na-abertura-da-79a-assembleia-geral-da-onu-em-nova-york. Acesso: 8 abr 2025.

MICROSOFT. **Microsoft Loves Linux**. 06 maio 2015. Microsoft Windows Server Blog. Disp. em: <https://www.microsoft.com/en-us/windows-server/blog/2015/05/06/microsoft-loves-linux>. Acesso em: 12 abr. 2025.

MICROSOFT. **AES Brasil colabora com a Microsoft na transição energética**. 31 ago. 2023. Disponível em: <https://news.microsoft.com/pt-br/aes-brasil-colabora-com-a-microsoft-na-transicao-energetica>. Acesso em: 12 abr. 2025.

MICROSOFT. **Sovereign Landing Zone**. 27 fev 2025a. Disponível em: <https://learn.microsoft.com/pt-br/azure/cloud-adoption-framework/ready/landing-zone/sovereign-landing-zone>. Acesso em: 09 abr 2025.

MICROSOFT. **Planeje e prepare-se para o Microsoft Cloud for Sovereignty no ciclo de lançamentos 1 de 2025**. 21 mar. 2025b. Disp. em: <https://learn.microsoft.com/pt-br/industry/release-plan/2025wave1/cloud-sovereignty/>. Acesso em: 09 abr. 2025.

NIC.br. **Conectividade significativa: propostas para medição e o retrato da população no Brasil**. Núcleo de Informação e Coordenação do Ponto BR; trad. Ana Zuleika Pinheiro Machado. S. Paulo, 2024.

OpenIA. **Introducing GPT-4o and more tools to ChatGPT free users.** In: OpenIa.com, 13 mai 2024. Disponível em: https://openai.com/index/gpt-4o-and-more-tools-to-chatgpt-free. Acesso em 7 abr 2025.

ORACLE. **Sovereign Cloud**. 2025. Disponível em: <https://www.oracle.com/br/cloud/sovereign-cloud>. Acesso em: 09 abr 2025.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 8 abr 2025.

_____. **Carta das Nações Unidas**, 26 de junho de 1945. Disponível em: https://www.oas.org/dil/port/1945%20Carta%20das%20Na%C3%A7%C3%B5es%20Unidas.pdf. Acesso em: 8 abr 2025.

_____. **Trust Territories Introduction.** UN Trusteeship Council Documentation, 2025. Disponível em: https://research.un.org/en/docs/tc/territories. Acesso em 8 abr 2025.

PORTUGAL, Ministério das Relações Exteriores. **Congresso de Vestefália.** PORTAL DIPLOMÁTICO. Disp. em: https://portaldiplomatico.mne.gov.pt/relacoes bilaterais/historia-diplomatica?view=article&id=520:congresso-de-vestefalia& catid=119. Acesso: 8 abr 2025.

SANTOS, Renan Gaya. **Infraestrutura Nacional de Dados.** Palestra para o portal ColaboraGov, em 14 ago 2024. Disponível em: https://www.youtube.com/watch?v=Fh4jgkzXujI. Acesso em: 13 abr 2025.

SÃO PAULO, Secretaria de Infraestrutura e Meio Ambiente do Estado de. **Consumo de energia elétrica no Estado de São Paulo em 2019.** [S.d.]. Disponível em: <https://dadosenergeticos.energia.sp.gov.br/PortalCEv2/intranet/Eletricidade/Distribuicao/ConsumoEstadoSP.asp?Ano=2019>. Acesso em: 09 abr. 2025.

SERPRO. **Aviso de Consulta Pública: Consulta Pública Eletrônica SUPGA/GACOM/GABSA nº 1863/2019.** Chamamento público para Procedimento de Solicitação de Proposta Técnica visando identificar Provedores de Serviços em Nuvem nas modalidades Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). Brasília, 2019. Disponível em: https://www.serpro.gov.br/consultas-publicas/sede/1863-2019. Acesso: 18 abr. 2025.

_____. **Serpro firma mais uma parceria para prestação de serviços em nuvem.** 2021a. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2021/parceria-nuvem>. Acesso em: 18 abr. 2025.

_____. **Serpro e Microsoft firmam parceria para serviços em nuvem.** 2021b. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2021/serpro-microsoft-nuvem>. Acesso em: 18 abr. 2025.

_____. **Serpro e Oracle firmam parceria em multicloud.** 2021c. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2021/serpro-e-oracle-firmam-parceria-em-multicloud>. Acesso em: 18 abr. 2025.

_____. **Serpro Nuvem Soberana**. 02 abr 2024a. Disp. em: <https://www.serpro.gov.br/menu/noticias/noticias-2024/serpro-nuvem-soberana>. Acesso em: 09 abr 2025.

_____. **Nuvem Serpro: Inteligência Artificial Nacional.** 31 jul. 2024b. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2024/nuvem-serpro-inteligencia-artificial-nacional. Acesso em: 13 abr. 2025.

_____. *Com novos clientes do poder judiciário, estados e municípios, Serpro Multicloud bate recorde de contratos em 2024*. Publicado em 15 jan 2025. Disp. em: https://www.serpro.gov.br/menu/noticias/noticias-2025/serpro-multicloud-novos-clientes. Acesso em: 19 abr. 2025.

_____. **Nuvem de Governo.** [s.d]. Disponível em: <https://loja.serpro.gov.br/nuvem-de-governo>. Acesso em: 18 abr. 2025.

SOFTEX. **Resumo Executivo – Indústria de Software e Serviços de TIC no Brasil: Caracterização e Trajetória Recente.** Observatório Softex, 2024. Disponível em: https://softex.br/observatorio/resumo-executivo-industria-de-software-e-servicos-de-tic-no-brasil-caracterizacao-e-trajetoria-recente/. Acesso em: 12 abr 2025.

USA – UNITED STATES OF AMERICA. Congress.Gov. **H.R.4922 - Communications Assistance for Law Enforcement Act,** 1994. Disponível em: https://www.congress.gov/bill/103rd-congress/house-bill/4922. Acesso: 22 abr 2025.

_____. **Bureau of Industry and Security. Supplement No. 1 to Part 740 - Country Groups.** Publicado em: 3 ago 2018. Disponível em: <https://www.bis.doc.gov/index.php/documents/regulations-docs/2255-supplement-no-1-to-part-740-country-groups-1>. Acesso em: 19 abr. 2025.

_____. Department of Justice. **CLOUD Act Resources**. 24 out 2023a. Disponível em: <https://www.justice.gov/criminal/cloud-act-resources>. Acesso em: 09 abr 2025.

_____. Office of the Director of National Intelligence. **Fisa Section 702 Fact Sheet**. 2023b. Disponível em: https://www.intelligence.gov/assets/documents/702%20Documents/FISA_Section_702_Fact_Sheet_JUN2023.pdf. Acesso em: 22 abr 2025.

_____. Federal Communications Commission. **Communications Assistance for Law Enforcement Act (CALEA).** 15 jan. 2025. Disponível em: <https://www.fcc.gov/calea>. Acesso em: 22 abr 2025.

_____. Department of Justice. **What is the Patriot Act.** [*s.d.*]. Disponível em: https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf. Acesso em: 22 abr 2025.

USA CALEA Act. Communications Assistance for Law Enforcement Act. Public Law 103-414, 108 Stat. 4279, 1994. Disponível em: https://www.congress.gov/103/statute/STATUTE-108/STATUTE-108-Pg4279.pdf. Acesso em: 8 abr 2025.

USA CLOUD Act. Clarifying Lawful Overseas Use of Data Act. Public Law 115–141, 132 Stat. 348, 2018. Disponível em: <https://www.congress.gov/bill/115th-congress/house-bill/4943>. Acesso em: 22 abr. 2025.

USA ECPA Act. Electronic Communications Privacy Act of 1986 (ECPA). Disponível em: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285>. Acesso em: 22 abr. 2025.

USA FISA - Foreign Intelligence Surveillance Act. 20 jun 2008. USA. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm. Acesso em: 22 abr 2025.

USA Freedom Act. 13 mai 2015. Disponível em: <https://judiciary.house.gov/usa-freedom-act>. Acesso em: 22 abr. 2025.

USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Public Law 107–56, 115 Stat. 272, 2001.

WAYMO. **Waymo and Uber expand partnership to bring autonomous ride-hailing to Austin and Atlanta**, 13 set 2024. Disponível em: https://waymo.com/blog/2024/09/waymo-and-uber-expand-partnership/ . Acesso em 19 jan 2025.

c) Publicações de Veículos de Imprensa e Portais de Internet

AFP. **Inteligência artificial: uma nova transformação para a guerra**. 16 nov 2023. UOL Notícias. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/afp/2023/11/16/inteligencia-artificial-uma-nova-transformacao-para-a-guerra.htm>. Acesso: 09 abr 2025.

___. **Trump anuncia projeto de IA "Stargate" com investimentos de "pelo menos US$ 500 bilhões" nos EUA.** UOL, 21 jan. 2025. Disponível em: https://noticias.uol.com.br/ultimas-noticias/afp/2025/01/21/trump-anuncia-projeto-de-ia-stargate-com-investimentos-de-pelo-menos-us-500-bilhoes-nos-eua.htm. Acesso em: 13 abr. 2025.

ALISSON, Elton. **SP concentra 55% das startups de base científica e tecnológica do país.** Agência Fapesp, 25 out. 2024. In: CNN Brasil. Disponível em: https://www.cnnbrasil.com.br/tecnologia/sp-concentra-55-das-startups-de-base-cientifica-e-tecnologica-do-pais/#:~:text=SP%20concentra%2055%25%20das%20startups%20de%20base%20cient%C3%ADfica%20e%20tecnol%C3%B3gica%20do%20pa%C3%ADs,-Levantamento%20identificou%20900&text=O%20Brasil%20possui%20hoje%20aproximadamente,(Pipe)%2C%20da%20Fapesp. Acesso em: 12 abr. 2025.

AL JAZEERA. **Google signs deal with startup to build small nuclear reactors to power AI**, 15 out 2024. Disponível em: https://www.aljazeera.com/economy/2024/10/15/google-signs-deal-with-startup-to-build-small-nuclear-reactors-to-power-ai . Acesso em 19 jan 2025.

BISCHOFF, Wesley. **Trump ameaça anexar Canadá e tomar Groenlândia e Canal do Panamá – o que está por trás disso**. 08 jan 2025. G1. Disponível em: <https://g1.globo.com/mundo/noticia/2025/01/08/trump-ameaca-anexar-canada-e-tomar-groenlandia-e-canal-do-panama-o-que-esta-por-tras-disso.ghtml>. Acesso: 09 abr 2025.

BLOOMBERG NEWS. **Análise: na guerra comercial contra a China, banir Huawei é a 'opção nuclear' de Trump.** Publicado em: 16 mai 2019. In: O Globo. Disponível em: https://oglobo.globo.com/economia/tecnologia/analise-na-guerra-comercial-contra-china-banir-huawei-a-opcao-nuclear-de-trump-23670227. Acesso em: 8 abr 2025.

BLOOMBERG. **E se a China invadir Taiwan? Ao menos as indústrias de chips da ilha já têm um plano B**. 22 mai 2024. In: O GLOBO. Disponível em: <https://oglobo.globo.com/economia/noticia/2024/05/22/e-se-a-china-invadir-taiwan-ao-menos-as-industrias-de-chips-da-ilha-ja-tem-um-plano-b.ghtml>. Acesso em: 09 abr 2025.

BURGESS, Matt. **Trump US cloud services Europe**, 24 mar. 2025. Wired. Disp. em: <https://www.wired.com/story/trump-us-cloud-services-europe>. Acesso em: 9 abr. 2025.

CAUTI, Carlo. **Entenda a ascensão e a possível queda das big techs chinesas.** 1º set 2021. Disponível em: <https://exame.com/invest/mercados/entenda-a-ascensao-e-a-possivel-queda-das-big-techs-chinesas/amp>. Acesso: 9 abr. 2025.

CARNAES, Mariana. **Estatais estrangeiras nas atividades estratégicas nacionais**. 21 jan. 2024. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2024-jan-21/estatais-estrangeiras-nas-atividades-estrategicas-nacionais>. Acesso em: 10 abr. 2025.

CCAF. **Cambridge Bitcoin Electricity Consumption Index – Comparisons**. [S.d.]. Disponível em: <https://ccaf.io/cbnsi/cbeci/comparisons>. Acesso em: 09 abr. 2025.

CLEMENTS, Thomas. **Zero Trust in the Trenches.** 13 fev. 2024. Disponível em: <https://www.secureworks.com/blog/zero-trust-in-the-trenches>. Acesso: 18 abr 2025

CNN BRASIL. **Governo quer liquidar Ceitec, empresa do 'chip de boi', antes de privatizações**. 07 jul. 2020. Disponível em: <https://www.cnnbrasil.com.br/economia/macroeconomia/governo-quer-liquidar-ceitec-empresa-do-chip-de-boi-antes-de-privatizacoes/>. Acesso em: 10 abr. 2025.

_____. **IBM impulsiona os negócios para se tornarem Data Driven**, 26 mai 2022. (Publieditorial) Disp. em: https://www.cnnbrasil.com.br/branded-content/tecnologia/ibm-impulsiona-os-negocios-para-se-tornarem-data-driven/ Acesso em 19 jan 2025.

_____. **Entenda o que é DeepSeek, IA que derrubou ações de tecnologia nesta segunda.** CNN Brasil, 27 jan. 2025. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/entenda-o-que-e-deepseek-ia-que-derrubou-acoes-de-tecnologia-nesta-segunda/. Acesso em: 13 abr. 2025.

COLLETTA, Ricardo Della. **Multilateralismo ameaçado**. 06 jun 2024. Folha de S.Paulo. Disponível em: <https://www1.folha.uol.com.br/mundo/2024/06/em-sp-lideres-do-the-elders-alertam-para-risco-de-erosao-do-sistema-multilateral.shtml>. Acesso em: 09 abr 2025.

COLLINS, Keith. **Julian Assange says tech companies asked WikiLeaks for details on alleged CIA exploits**. Quartz, 9 mar. 2017. Disponível em: <https://qz.com/928966/julian-assange-says-tech-companies-asked-wikileaks-for-details-on-alleged-cia-exploits>. Acesso em: 9 abr. 2025.

CONVERGÊNCIA DIGITAL. **Serpro firma contrato sem licitação de R$ 71,2 milhões com a AWS.** 23 mar. 2020. Disp. em: <https://convergenciadigital.com.br/governo/serpro-firma-contrato-sem-licitacao-de-r-712-milhoes-com-a-aws>. Acesso em: 18 abr. 2025.

_____. **Serpro inclui IBM em oferta de multicloud com acordo de R$ 403 milhões.** 1º fev 2022. Disponível em: <https://convergenciadigital.com.br/especial/cloud/serpro-inclui-ibm-em-oferta-de-multicloud-com-acordo-de-r-403-milhes/>. Acesso em: 18 abr. 2025.

CORREIA, Victor. **Lula lança Plano Brasileiro de Inteligência Artificial nesta terça. Correio Braziliense**, 29 jul. 2024. Disponível em: https://www.correiobraziliense.com.br/politica/2024/07/6908525-lula-lanca-plano-brasileiro-de-inteligencia-artificial-nesta-terca.html. Acesso em: 13 abr. 2025.

COUTINHO, Mateus. **Lula cita ameaça de 'colonialismo digital' e defende regulação das redes.** 17 mar 2025. Portal UOL. Disp: em: https://noticias.uol.com.br/politica/ultimas-noticias/2025/03/17/lula-oab-posse.htm. Acesso em: 8 abr 2025.

COUTURE, Stéphane; TOUPIN, Sophie. **What Does the Concept of 'Sovereignty' Mean in Digital, Network and Technological Sovereignty?** In: GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017. Publicado em 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107272. Acesso 8 abr 2025.

DESMARAIS, Anna. **Poderão os EUA desativar as armas europeias? Especialistas avaliam receio do "kill switch".** Euronews Next, 13 mar. 2025. Disponível em: <https://pt.euronews.com/next/2025/03/13/poderao-os-eua-desativar-as-armas-europeias-especialistas-avaliam-receio-do-kill-switch>. Acesso em: 20 abr. 2025.

ESQUERDA.NET. **Bloco propõe uma agência portuguesa para soberania digital.** Disponível em: <https://www.esquerda.net/artigo/bloco-propoe-uma-agencia-portuguesa-para-soberania-digital/93890>. Publicado em: 16 fev. 2025, 12h59. Acesso em: 9 abr. 2025.

EURONEWS. **Amazon follows Google in taking the nuclear option to power data centres**. 17 out. 2024. Disponível em: <https://www.euronews.com/business/2024/10/17/amazon-follows-google-in-taking-the-nuclear-option-to-power-data-centres>. Acesso em: 09 abr. 2025.

EXAME. **Com restrição à mineração na China, consumo energético do Bitcoin despenca**. 25 jun. 2021. Disponível em: <https://exame.com/future-of-money/criptoativos/com-restricao-a-mineracao-na-china-consumo-energetico-do-bitcoin-despenca>. Acesso em: 09 abr. 2025.

FALCÃO, Arthur; BUSTAMANTE, Anna. **'Derrota para Musk': como a imprensa internacional repercutiu a volta da rede X ao Brasil.** In: O Globo, 9 out 2024. Disp. em: https://oglobo.globo.com/brasil/noticia/2024/10/09/derrota-para-musk-como-a-imprensa-internacional-repercutiu-a-volta-da-rede-x-ao-brasil.ghtml. Acesso em: 8 abr 2025.

FAUSTINO, Rafael. **Uber já oferece carros sem motorista nos EUA, 27 out 2023. Época Negócios.** Disp. em: https://epocanegocios.globo.com/tecnologia/noticia/2023/10/uber-ja-oferece-carros-sem-motorista-nos-eua.ghtml . Acesso: 19 jan 2025.

FINANCIAL TIMES. **EUA propõem proibição de software e componentes chineses em veículos.** Publicado em: 23 set 2024. In: Folha. Disponível em: https://www1.folha.uol.com.br/mercado/2024/09/eua-propoem-proibicao-de-software-e-componentes-chineses-em-veiculos.shtml. Acesso em: 8 abr 2025.

FONSECA, Enio; MICHELLIS JR., Decio. **A nuvem devoradora de energia. In: portal Direito Ambiental.** 2 mar 2023. Disponível em: https://direitoambiental.com/a-nuvem-devoradora-de-energia/ . Acesso em 19 jan 2025.

FORTUNE BUSINESS INSIGHTS. **Server Operating System Market Size**. 24 Mar 2025. Fortune Business Insights. Disponível em: <https://www.fortunebusinessinsights.com/server-operating-system-market-106601>. Acesso em: 12 abr. 2025.

FREITAS, Camilla. **Energia elétrica no Brasil não é privatizada; saiba o motivo.** 06 nov. 2024. UOL Economia. Disponível em: <https://economia.uol.com.br/noticias/redacao/2024/11/06/energia-eletrica-no-brasil-nao-e-privatizada-saiba-o-motivo.htm>. Acesso em: 10 abr. 2025.

GATTO, Gabriel. **Comitê da Câmara dos EUA aprova 'lei anti-Moraes' para barrar estrangeiros acusados de promover censura**. 26 fev 2025. Portal TERRA. Disponível em: <https://www.terra.com.br/noticias/mundo/estados-unidos/comite-da-camara-dos-eua-aprova-lei-anti-moraes-para-barrar-estrangeiros-acusados-de-promover-censura,c187db90e4399c71ebca15e090566c037z9fnh8r.html>. Acesso em: 09 abr 2025.

G1. **Agência de comunicações dos EUA aprova plano para substituir equipamentos da Huawei e ZTE.** Publicado em: 14 jul 2021. Disp. em: https://g1.globo.com/economia/tecnologia/noticia/2021/07/14/agencia-de-comunicacoes-dos-eua-aprova-plano-para-substituir-equipamentos-da-huawei-e-zte.ghtml. Acesso em: 8 abr 2025.

G1. **Tarifaço de Trump: taxa de 104% contra a China entra em vigor nesta quarta-feira**. 09 abr 2025. Disponível em: <https://g1.globo.com/economia/noticia/2025/04/09/tarifaco-de-trump-taxa-de-104percent-contra-a-china-entra-em-vigor-nesta-quarta-feira.ghtml>. Acesso em: 09 abr 2025.

GARDNER, Frank. **Como o ano das guerras uniu rivais e criou novos inimigos – e o que esperar de 2025.** 02 jan 2025. G1. Disponível em: <https://g1.globo.com/mundo/noticia/2025/01/02/como-o-ano-das-guerras-uniu-rivais-e-criou-novos-inimigos-e-o-que-esperar-de-2025.ghtml>. Acesso: 09 abr 2025.

GREENWALD, Glenn; MACASKILL, Ewen. **US tech giants NSA data.** The Guardian, 7 jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 9 abr. 2025.

GROSSMANN, Luís Osvaldo. **Trump mira satélites, taxação de big techs e LGPD para incluir Brasil em tarifaço**. 02 abr 2025a. In: CONVERGÊNCIA DIGITAL. Disponível em: <https://convergenciadigital.com.br/governo/trump-mira-satelites-taxacao-de-big-techs-e-lgpd-para-incluir-brasil-em-tarifaco/>. Acesso: 09 abr 2025.

_____. **Serpro aciona Nuvem Soberana: cofres são das big techs, mas só o governo tem a chave.** Convergência Digital, 20 fev. 2025b. Disp. em: <https://convergenciadigital.com.br/governo/exclusivo-serpro-aciona-nuvem-soberana-cofres-sao-das-big-techs-mas-so-o-governo-tem-a-chave/>. Acesso em: 19 abr. 2025.

HAWKINS, M.; BLOOMBERG. **U.S. preps China chip curbs that stop short of early proposals.** Fortune, 27 nov. 2024. Disponível em: https://fortune.com/asia/2024/11/27/us-preps-china-chip-curbs-that-stop-short-of-early-proposals. Acesso em: 9 abr. 2025.

JOSÉ, Pedro. **Brasil enfrenta apagão de profissionais de TI**. 24 ago. 2024. Correio Braziliense. Disponível em: <https://www.correiobraziliense.com.br/economia/2024/08/6927263-brasil-enfrenta-apagao-de-profissionais-de-ti.html>. Acesso em: 12 abr. 2025.

KEMP, Simon. **Digital 2025: Brazil**. 3 mar 2025. DataReportal. Disponível em: <https://datareportal.com/reports/digital-2025-brazil>. Acesso em: 12 abr 2025.

KNOTH, Pedro. **AT&T conclui venda da Sky Brasil e Directv Go após prejuízo bilionário**. Tecnoblog, 2021. 29 dez. 2023. Disponível em: https://tecnoblog.net/noticias/att-conclui-venda-da-sky-brasil-e-directv-go-apos-prejuizo-bilionario. Acesso em: 10 abr 2025.

KOROTAEV, Mikhail. **Why the AWS European Sovereign Cloud is an obstacle to reaching true digital sovereignty.** 26 out. 2023. Disponível em: <https://nextcloud.com/blog/why-aws-is-an-obstacle-to-true-digital-sovereignty/>. Acesso em: 18 abr. 2025.

KREMPL, Stefan. **Blackmailability concerns: Computer scientists oppose BSI-Google cloud deal.** Heise Online, 21 mar. 2025, 21h06 CET. Disponível em: <https://www.heise.de/en/news/Blackmailability-concerns-Computer-scientists-oppose-BSI-Google-cloud-deal-10325001.html>. Acesso em: 9 abr. 2025.

LANDAU, Susan. **CALEA Was a National Security Disaster Waiting to Happen.** 13 nov 2024. Disponível em: <https://www.lawfaremedia.org/article/calea-was-a-national-security-disaster-waiting-to-happen>. Acesso em: 22 abr. 2025.

LENDON, Brad. **Otan pode sobreviver sem apoio dos Estados Unidos, dizem analistas**. 07 mar 2025. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/internacional/otan-pode-sobreviver-sem-apoio-dos-estados-unidos-dizem-analistas>. Acesso em: 09 abr 2025.

LIMA, Thiago. **Power struggle: will Brazil's booming datacentre industry leave ordinary people in the dark?** *The Guardian*, 04 Mar 2025. Disponível em: <https://www.theguardian.com/global-development/2025/mar/04/brazil-power-electricity-energy-poverty-datacentre-boom>. Acesso em: 12 abr. 2025.

MARTÍNEZ-VARGAS, Ivan. **Brasil já colhe benefícios do boom dos data centers.** 06 nov. 2024. Valor Econômico, de São Paulo. Disponível em: <https://valor.globo.com/publicacoes/especiais/investimento-estrangeiro/noticia/2024/11/06/brasil-ja-colhe-beneficios-do-boom-dos-data-centers.ghtml>. Acesso em: 11 abr. 2025.

MIATO, Bruna. **Brasil volta ao grupo das 10 maiores economias do mundo com resultado do PIB de 2023**, 1 mar 2024. In: G1 Economia. Disponível em: https://g1.globo.com/economia/noticia/2024/03/01/brasil-volta-ao-grupo-das-10-maiores-economias-do-mundo-com-resultado-do-pib-de-2023.ghtml Acesso em 19 jan 2025.

MOHAMMED, A.; LAWDER, D.; FREIFELD, K. **US Expands Russia Sanctions, Targets Chips Sent Via China.** U.S. News, 12 jun. 2024. Disponível em: https://www.usnews.com/news/world/articles/2024-06-12/us-widens-russia-sanctions-targets-semiconductors-sent-via-china. Acesso em: 9 abr. 2025.

MOLINARO, Domenic. **O que é um ataque de força bruta?** *Avast*. Atualizado em 08 abr. 2024. Disponível em: https://www.avast.com/pt-br/c-what-is-a-brute-force-attack. Acesso em: 19 abr. 2025.

MURPHY, Andrea; SCHIFRIN, Matt. **Global 2000: conheça as 10 maiores empresas listadas do mundo em 2024**, 13 jun 2024. In: Forbes. Disponível em: https://forbes.com.br/forbes-money/2024/06/global-2000-conheca-as-10-maiores-empresas-listadas-do-mundo-em-2024/#foto4 . Acesso em 19 jan 2025.

O GLOBO. **Israel usou IA para definir 37 mil alvos, com cálculo de 'permissão prévia' de morte de civis, diz investigação**, 4 abr 2024a. Disponível em: https://oglobo.globo.com/mundo/noticia/2024/04/04/israel-usou-ia-para-definir-37-mil-alvos-com-calculo-de-permissao-previa-de-morte-de-civis-diz-investigacao.ghtml Acesso em 19 jan 2025.

O GLOBO. **Israel pôs explosivos nas baterias dos pagers de forma tão sofisticada que ficaram indetectáveis, dizem autoridades do Líbano.** *O Globo*, 27 set. 2024b. Disponível em: <https://oglobo.globo.com/mundo/noticia/2024/09/27/israel-pos-explosivos-nas-baterias-dos-pagers-de-forma-tao-sofisticada-que-ficaram-indetectaveis-dizem-autoridades-do-libano.ghtml>. Acesso em: 9 abr. 2025.

PADINGER, Germán. **Entenda o crescimento da extrema-direita na Europa nos últimos anos**. 26 set 2022. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/internacional/entenda-o-crescimento-da-extrema-direita-na-europa-nos-ultimos-anos/>. Acesso em: 09 abr 2025.

PISTONO, Rafael. **Compartilhamento de postes e o perigo da criatividade legislativa**. Teletime, [S. l.], 22 nov. 2024. Disponível em: https://teletime.com.br/22/11/2024/compartilhamento-de-postes-e-o-perigo-da-criatividade-legislativa/. Acesso: 10 abr. 2025.

PODER360. **Saída da Starlink pode causar prejuízos, disse a Defesa em junho.** Publicado em 30 ago 2024a. Disp. em: https://www.poder360.com.br/poder-tech/saida-da-starlink-pode-causar-prejuizos-disse-a-defesa-em-junho. Acesso em: 8 abr 2025

PODER360. **20% das empresas fecham ainda no 1º ano no Brasil, diz IBGE**. 5 dez 2024b. Disponível em: <https://www.poder360.com.br/poder-empreendedor/20-das-empresas-fecham-no-1o-ano-no-brasil-diz-ibge/>. Acesso em: 12 abr 2025.

PPLWARE. **Os satélites Starlink da SpaceX têm câmaras?** Publicado em 11 abr 2024. Disponível em: https://pplware.sapo.pt/high-tech/os-satelites-starlink-da-spacex-tem-camaras. Acesso em: 8 abr 2025

REUTERS. **China warns of 'necessary actions' if US escalates chip curbs.** *Reuters*, 28 nov. 2024a. Disponível em: <https://www.reuters.com/markets/china-warns-necessary-actions-if-us-escalates-chip-curbs-2024-11-28>. Acesso em: 9 abr. 2025.

REUTERS. **Entenda a disputa entre Elon Musk e o Supremo Tribunal Federal**. 29 ago 2024b. In: INFOMONEY. Disponível em: <https://www.infomoney.com.br/politica/entenda-a-disputa-entre-elon-musk-e-o-supremo-tribunal-federal>. Acesso em: 09 abr 2025.

REUTERS. **China proíbe mineração e declara ilegais transações com criptomoedas no país**. 24 set. 2021. Disponível em: <https://www.cnnbrasil.com.br/economia/financas/china-amplia-restricoes-e-proibe-mineracao-de-criptomoedas-em-todo-o-pais/>. Acesso em: 09 abr. 2025.

RODRIGUES, Lays. **Os 29 principais projetos de data centers lançados em 2023 na América Latina.** DatacenterDynamics, 07 dez. 2023. Disponível em: <https://www.datacenterdynamics.com/br/an%C3%A1lises/os-29-principais-projetos-de-data-centers-lancados-em-2023-na-america-latina/>. Acesso em: 11 abr. 2025.

ROGOWAY, Mike. **Google's water use is soaring in The Dalles, records show, with two more data centers to come**, 2022. In: The Oregonian/OregonLive. Disponível em: https://www.oregonlive.com/silicon-forest/2022/12/googles-water-use-is-soaring-in-the-dalles-records-show-with-two-more-data-centers-to-come.html Acesso: 19 jan 2025.

ROSA, Alexandre Morais da; VIEIRA, Marília Raposo. **Cloud Act: Quando a investigação se dá nas nuvens americanas.** Consultor Jurídico, 22 nov. 2019. Disponível em: <https://www.conjur.com.br/2019-nov-22/limite-penal-cloud-act-quando-investigacao-nuvens-americanas/>. Acesso em: 22 abr. 2025.

SALATIEL, José Renato. **Censura à internet - Google fecha as portas na China comunista**. Especial para a Página 3 Pedagogia & Comunicação. 2025. Disponível em: <https://vestibular.uol.com.br/resumo-das-disciplinas/atualidades/censura-a-internet-google-fecha-as-portas-na-china-comunista.htm>. Acesso em: 9 abr. 2025.

SAMPAIO, Henrique. **TikTok banido nos EUA? Entenda o que pode acontecer com a rede social no Brasil.** Publicado em: 25 abr 2024. In: CNN Brasil. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/tiktok-banido-nos-eua-entenda-o-que-pode-acontecer-com-a-rede-social-no-brasil. Acesso em 8 abr 2025.

SANT'ANA, Jéssica. **Anatel autoriza venda da Oi Móvel para consórcio formado por Claro, Tim e Vivo.** G1, Brasília, 31 jan. 2022. Disponível em: https://g1.globo.com/economia/noticia/2022/01/31/anatel-autoriza-venda-da-oi-movel-para-consorcio-formado-por-claro-tim-e-vivo.ghtml. Acesso em: 10 abr. 2025.

SÉRVIO, Gabriel. **Anatel decide futuro da Starlink no Brasil esta semana; entenda**. Olhar Digital, 31 mar. 2025. Disponível em: https://olhardigital.com.br/2025/03/31/pro/anatel-decide-futuro-da-starlink-no-brasil-esta-semana-entenda/. Acesso: 10 abr. 2025.

SHERMAN, Natalie. **Microsoft chooses infamous nuclear site for AI power**, em 24 set 2024. In: BBC News. Disponível em: bbc.com/news/articles/cx25v2d7zexo. Acesso em: 19 jan 2025.

SIC NOTÍCIAS. **Corredor econômico Índia-Médio Oriente-Europa: uma alternativa à rota da seda da China**. 10 set 2023. Disponível em: <https://sicnoticias.pt/mundo/2023-09-10-Corredor-economico-India-Medio-Oriente-Europa-uma-alternativa-a-rota-da-sede-da-China-e8d44d3a>. Acesso: 09 abr 2025.

SKELTON, Sebastian Klovig. **Microsoft admits no guarantee of sovereignty for UK policing data.** Computer Weekly, 19 jun. 2024. Disponível em: <https://www.computerweekly.com/news/366589152/Microsoft-admits-no-guarantee-of-sovereignty-for-UK-policing-data>. Acesso em: 9 abr. 2025.

SOUZA, Beto. **Enel levou 6 dias para restabelecer luz em 2023 em SP; apagão de agora já dura 3 dias**. 14 out. 2024. CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/nacional/enel-levou-6-dias-para-restabelecer-luz-em-2023-em-sp-apagao-de-agora-ja-dura-3-dias>. Acesso em: 10 abr. 2025.

THE GUARDIAN. **NSA inspector general report on email and internet data collection under Stellar Wind – full document.** *The Guardian*, 27 jun. 2013. Disponível em: <https://www.theguardian.com/nsa-inspector-general-report-document-data-collection>. Acesso em: 9 abr. 2025.

TI INSIDE. **Justiça do Trabalho adota serviços multicloud do Serpro.** Publicado em: 14 abr. 2025. Disponível em: <https://tiinside.com.br/14/04/2025/justica-do-trabalho-adota-servicos-multicloud-do-serpro/>. Acesso em: 19 abr. 2025.

UM SÓ PLANETA. **Queima de combustíveis fósseis representa 87% das emissões globais de CO2, diz relatório**, em 10 ago 2023. In: Globo.com. Disponível em: https://umsoplaneta.globo.com/energia/noticia/2023/08/10/queima-de-combustiveis-fosseis-representa-87percent-das-emissoes-globais-de-co2-diz-relatorio.ghtml . Acesso19 jan 2025.

VAIDHYANATHAN, Siva. **Elon Musk's Real Threat to Democracy Isn't What You Think. How the attention-starved CEO took over our communications infrastructure.** The Nation, em 11 dez 2023. Disponível em: https://www.thenation.com/article/society/elon-musk-democracy-threat. Acesso em: 8 abr 2025.

VANIAN, Jonathan. **How digital surveillance thrived in the 20 years since 9/11.** Publicado em: 8 set 2021. In: Fortune. Disp. em: https://fortune.com/2021/09/08/digital-privacy-patriot-act-9-11. Acesso em: 8 abr 2025.

VERNALHA, Fabrício. **Privacidade de dados e segurança cibernética na gestão.** LinkedIn, 12 jun. 2023. Disponível em: <https://www.linkedin.com/pulse/privacidade-de-dados-e-seguran%C3%A7a-cibern%C3%A9tica-na-gest%C3%A3o-vernalha>. Acesso em: 19 abr. 2025.

VIDAL, Iara. **China chama a EUA de abutre cibernético por espionar celulares no mundo inteiro**, 25 mar. 2025. Revista Fórum. Disp. em: <https://revistaforum.com.br/global/chinaemfoco/2025/3/25/china-chama-eua-de-abutre-cibernetico-por-espionar-celulares-no-mundo-inteiro-176308.html>. Acesso em: 9 abr. 2025.

VILLAVERDE, Adão. **Os semicondutores e a geopolítica mundial.** *GZH*, 27 nov. 2024. Disp. em: <https://gauchazh.clicrbs.com.br/opiniao/noticia/2024/11/os-semicondutores-e-a-geopolitica-mundial-cm3yxmrah00iw013bmqw3dmjc.html>. Acesso em: 9 abr. 2025.

WONG, Tessa. **A nova rota da seda que a China quer construir vale o investimento trilionário?**. 18 out 2023. BBC News. Disponível em: <https://www.bbc.com/portuguese/articles/cmj544lg205o>. Acesso em: 09 abr 2025.