Soberania Digital no Brasil

Diagnóstico, Desafios e Caminhos sob a perspectiva da Ciência, Tecnologia e Inovação (Sumário Executivo Estendido)

Centro de Gestão e Estudos Estratégicos
Ciência, Tecnologia e Inovação

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Sumário Executivo Estendido - Soberania digital no brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação

Equipe técnica do MCTI

Henrique de Oliviera Miguel (*Secretário de Ciência, Tecnologia e Inovação para a Transformação Digital – SETAD/MCTI)*

Hugo Valadares *(Diretor - DECTI)*

Eliana Cardoso Emediato *(Coordenadora-Geral - CGGD)*

André Rafael Costa e Silva *(Coordenador - COPID)*

Adriana Anunciatto Depieri (*Analista em Ciência e Tecnologia)*

Daniel Boson *(Especialista em Políticas Públicas e Gestão Governamental)*

Amauri Casarin Junior (*Analista em Ciência e Tecnologia)*

Equipe técnica do CGEE

Caetano Christophe Rosado Penna (*Diretor supervisor*)

Caroline Nascimento Pereira (*Líder de projeto*)

Isabela Quadros Dantas Barros

Consultor técnico

Luca Belli (FGV-RJ)

SUMÁRIO

1. CONTEXTO E JUSTIFICATIVA

A soberania digital emerge como questão estratégica fundamental para o Brasil no século XXI. Em um cenário global marcado pela concentração tecnológica, dependências estruturais e disputas geopolíticas pelo controle de infraestruturas e dados, a capacidade de exercer autodeterminação na esfera digital tornou-se elemento essencial da soberania nacional. O Brasil possui ativos relevantes, comunidade científica qualificada, marcos regulatórios avançados como a LGPD e o Marco Civil da Internet, base industrial diversificada e infraestrutura de pesquisa reconhecida internacionalmente. No entanto, enfrenta fragilidades críticas: dependência de tecnologias estrangeiras em várias dimensões, subinvestimento em P&D, fragmentação institucional, lacunas em áreas estratégicas como semicondutores e computação de alto desempenho, e dependências em elementos essenciais como computação em nuvem e sistemas de IA.

Diante deste cenário, a presente nota técnica introduz os fundamentos conceituais, institucionais e tecnológicos da soberania digital brasileira e propõe diretrizes para o desenvolvimento de um ecossistema digital nacional capaz de fortalecer a autonomia tecnológica. Com base nas definições elaboradas pela literatura especializada, o documento defende que a soberania digital deve ser compreendida como a capacidade de entender o funcionamento, desenvolver e regular efetivamente tecnologias digitais. Essa capacidade é fundamental para que o Estado exerça controle jurídico, técnico e operacional sobre infraestruturas críticas e sistemas digitais que sustentam o funcionamento da sociedade, da economia e da democracia brasileiras. Nessa perspectiva, **a soberania digital não é sinônimo de autarquia digital, mas deve ser compreendida como a capacidade de entender o funcionamento, desenvolver e regular efetivamente tecnologias digitais** e configura-se como elemento central para a preservação do direito à autodeterminação informacional, tanto em sua dimensão individual quanto coletiva.

O diagnóstico apresentado evidencia que o Brasil possui importantes ativos institucionais e científicos, mas enfrenta problemas e dependências significativas em várias dimensões, conforme supracitado, que limitam a autonomia nacional e expõem o país a riscos geopolíticos, econômicos e da manutenção e uso coercitivo de dependências tecnológicas. Nesta perspectiva, a CT&I assumem papel estratégico, que precisa ser explorado de maneira mais assertiva como elemento propulsor da soberania digital brasileira, para articular a construção de um ecossistema digital tecnologicamente autônomo, aberto e cooperativo. Como demonstram as experiências internacionais analisadas, o uso estratégico da CT&I representa o elemento comum às trajetórias bem-sucedidas.

À luz das análises apresentadas, as recomendações convergem para um objetivo central: alavancar a transformação digital como vetor de desenvolvimento econômico, inclusão social e autonomia tecnológica, articulando infraestrutura, ciência, indústria e governança em um projeto nacional de longo prazo. Por fim, reconhecendo a complexidade temática, a nota destaca a necessidade de se analisar de maneira pormenorizada as dimensões examinadas, identificando áreas mais relevantes a serem priorizadas no curto e médio prazo e estabelecer métricas para monitorar avanços em tais áreas.

2. DIAGNÓSTICO: CAPACIDADES E DESAFIOS

O cenário brasileiro de soberania digital caracteriza-se por uma combinação de ativos estratégicos relevantes e gargalos estruturais persistentes que limitam a autonomia tecnológica nacional. Entre as principais **vantagens comparativas** do país destacam-se a existência de setores econômicos com elevada intensidade informacional e grande potencial de aplicação de tecnologias digitais avançadas,

como saúde, finanças, educação, agronegócio, energia, mineração e petróleo e gás. Esses setores reúnem grandes volumes de dados, demanda tecnológica sofisticada e capacidade de indução de inovação, configurando-se como alavancas centrais para o desenvolvimento de soluções digitais nacionais, inclusive em IA. Soma-se a esse quadro uma matriz energética majoritariamente renovável, fator estratégico em um contexto global no qual *data centers*, supercomputadores e sistemas de IA demandam volumes crescentes de energia e enfrentam crescentes restrições ambientais e regulatórias. **Além de amplas reservas de minerais críticos, essenciais para a produção de hardware e a transição energética global.**

Apesar desses ativos, o diagnóstico evidencia **gargalos estruturais** como o **subfinanciamento crônico da CT&I e a falta de visão orgânica,** especialmente nas áreas digitais, afetando a continuidade de projetos estruturantes, a retenção de talentos e impedindo a consolidação de capacidades industriais em *hardware*, *software* e infraestrutura computacional. A dependência de *hardware* estrangeiro, notadamente de semicondutores avançados, GPUs e equipamentos de rede baseados em arquiteturas proprietárias, expõe o país a riscos geopolíticos, econômicos e operacionais, além de impor custos elevados e restrições ao desenvolvimento de modelos avançados de IA e aplicações científicas de alto desempenho. No plano **infraestrutural**, observa-se um ecossistema fragmentado de computação em nuvem e de processamento de alto desempenho, com iniciativas operando de forma pouco coordenada, com arquiteturas heterogêneas, baixa interoperabilidade e forte dependência de provedores estrangeiros. A escassez de GPUs de última geração e a ausência de aquisições coordenadas de *hardware* acelerador comprometem tanto a pesquisa científica quanto a inovação industrial, dificultando a criação de *clusters* nacionais capazes de sustentar projetos de grande escala em IA, como modelagem climática, bioinformática , etc.

A **desarticulação institucional** é um grave problema, com fragmentação da governança e ausência de uma autoridade central com competência para coordenar políticas de infraestruturas, sistemas de IA, cibersegurança e resiliência cibernética. Diversos órgãos exercem atribuições sobre aspectos relacionados à autonomia tecnológica, mas sem mecanismos de coordenação efetivos. Do ponto de vista social, o quadro é agravado pela desigualdade no acesso à conectividade significativa, em que apenas 22% da população brasileira dispõe de conectividade significativa. A prevalência de planos móveis restritivos e de práticas como o *zero rating* concentra artificialmente a atenção dos usuários da internet em um conjunto limitado de plataformas patrocinadas, reforçando dependências tecnológicas, distorcendo a concorrência e limitando o potencial da transformação digital como vetor de inclusão social e desenvolvimento econômico.

3. FUNDAMENTOS: DIMENSÕES DA SOBERANIA DIGITAL

A soberania digital é compreendida, nesta nota, como uma condição multidimensional que envolve a capacidade de compreender, desenvolver, escolher e regular tecnologias digitais de forma alinhada aos interesses nacionais e aos princípios constitucionais. Essa condição se manifesta em diferentes dimensões interdependentes, cuja fragilidade em qualquer camada compromete a autonomia do conjunto.

A **dimensão informacional** refere-se ao controle sobre fluxos de dados pessoais, governamentais, científicos e industriais, bem como à garantia de que dados estratégicos estejam submetidos à jurisdição nacional. Embora o Brasil disponha de um marco legal avançado de proteção de dados, a dependência de serviços de nuvem estrangeiros, frequentemente sujeitos a legislações extraterritoriais,

cria vulnerabilidades que esvaziam a autodeterminação informacional na prática. A soberania informacional exige, portanto, não apenas normas jurídicas, mas também infraestruturas nacionais capazes de armazenar e processar dados (sensíveis) com segurança e ser auditáveis com transparência. Por sua vez, a **dimensão infraestrutural** diz respeito ao controle sobre os ativos físicos que sustentam o ecossistema digital, a partir de semicondutores e incluindo redes de telecomunicações, cabos submarinos, *data centers*, nuvens computacionais e sistemas de alto desempenho. O domínio dessas infraestruturas é condição essencial para a continuidade de serviços públicos, a segurança nacional e a competitividade econômica. A concentração global dessas estruturas em poucos países e empresas torna Estados dependentes vulneráveis a interrupções, aumentos de custos e pressões geopolíticas.

A **dimensão lógica** envolve o domínio sobre software, algoritmos, modelos, bibliotecas e padrões técnicos que definem o funcionamento das tecnologias digitais. A dependência de soluções proprietárias estrangeiras limita a auditabilidade, a interoperabilidade e a capacidade de adaptação às necessidades nacionais, enquanto aumenta a extração de renda de maneira despropositada. Nesse contexto, o uso estratégico de software livre, padrões abertos, tecnologias em *open source* e modelos auditáveis emerge como instrumento central de soberania prática, permitindo reduzir *lock-ins* tecnológicos e ampliar estrategicamente a capacidade regulatória efetiva do Estado. A **cibersegurança, ciberdefesa e segurança nacional** constitui dimensão transversal e indissociável da soberania digital. A proteção de infraestruturas críticas, dados pessoais (sensíveis) e confidenciais e sistemas de IA contra-ataques, espionagem e interferência externa depende do domínio técnico sobre a própria arquitetura tecnológica nacional, pois sem autonomia para compreender, auditar e governar esses ativos torna-se impossível mapear as vulnerabilidades ou formular políticas eficazes de resiliência. A terceirização excessiva da cibersegurança para fornecedores estrangeiros, cujos códigos e arquiteturas não são plenamente auditáveis, cria vetores de risco que transcendem a esfera técnica e alcançam os planos jurídico e geopolítico, expondo o país a riscos de espionagem, sabotagem e coerção. Para superar esse quadro, é necessário combinar um marco jurídico robusto, uma Agência de Cibersegurança com autonomia operacional e políticas industriais, educacionais e tecnológicas que fomentem soluções nacionais em áreas como semicondutores, criptografia, nuvem e IA, fazendo da soberania digital, ao mesmo tempo, uma política de segurança nacional e de desenvolvimento econômico.

Por fim, a nota incorpora o conceito de **interdependência instrumentalizada**, que descreve como a concentração de posições estratégicas em redes globais permite a exploração coercitiva de dependências. A doutrina associas a este conceito as chamados efeitos panópticos, que permitem à capacidade de vigilância e extração de informação, e efeitos de estrangulamento, ligados ao controle de gargalos críticos, representam riscos concretos para países que não dominam cadeias de suprimento e infraestruturas digitais essenciais.

4. PAPEL DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO (CT&I)

A CT&I são prioridades nacionais nos países tecnologicamente mais avançados, constituindo um dos principais vetores de competitividade econômica, soberania digital, cibersegurança e segurança nacional, permitindo alcançar maior autonomia tecnológica. Esse entendimento estruturou ecossistemas robustos de universidades, centros de pesquisa, empresas de base tecnológico, permitindo avanços científicos e a consolidação de autonomia tecnológica em áreas críticas. Tal

dinâmica pode ser observada em países como Estados Unidos, Japão, Coreia do Sul, China e Israel, nos quais a CT&I possui destaque.

No atual contexto digital, marcado pela convergência entre elementos tecnológicos, geopolíticos e geoeconômicos, a centralidade da CT&I torna-se ainda mais evidente, dado o caráter da CT&I como determinante. Nesse contexto, o **Ministério da Ciência, Tecnologia e Inovação (MCTI) apresenta papel determinante como articulador central do ecossistema nacional**, tendo a responsabilidade para organizar e integrar diversos atores do sistema a partir de uma visão estratégica compartilhada, capaz de alinhar esforços e recursos em torno de objetivos comuns. Assim como sobre a facilitação e criação de alianças setoriais e o monitoramento das ações voltadas ao aprimoramento da soberania digital.

A **Estratégia Nacional de Ciência, Tecnologia e Inovação** (ENCTI 2024–2034) representa avanço relevante ao reconhecer explicitamente a transformação digital como vetor transversal do desenvolvimento brasileiro. Ademais, indica a necessidade de reduzir dependências tecnológicas críticas, fortalecer capacidades endógenas e integrar CT&I às políticas industriais e sociais. Por sua vez, o **Plano Brasileiro de Inteligência Artificial (PBIA)** complementa essa visão ao estabelecer diretrizes para infraestrutura computacional, dados, formação de talentos e governança de IA. O PBIA reconhece que a ausência de capacidade nacional de processamento de alto desempenho compromete a pesquisa científica e a adoção soberana de sistemas de IA.

Nesse cenário, o **Sistema Nacional de Processamento de Alto Desempenho (SINAPAD)** emerge como ativo estratégico, tanto no apoio à pesquisa, quanto na formação de recursos humanos, no desenvolvimento de produtos e serviços nacionais de HPC e na sustentação de ecossistemas de IA e ciência orientada por dados. Contudo, para cumprir esse papel, é necessário financiamento previsível, governança integrada e articulação com políticas digitais e industriais.

5. LIÇÕES DAS EXPERIÊNCIAS INTERNACIONAIS

A análise comparada de experiências internacionais demonstra que a soberania digital não resulta de ações isoladas, mas de estratégias integradas que articulam Estado, indústria, ciência e infraestrutura. Nos **Estados Unidos**, o Estado atua como cliente âncora por meio de compras públicas estratégicas e políticas industriais, como *o Buy American Act,* determinante para a expansão do mercado de *cloud computing* doméstico, fortalecendo a posição dominante dos *hyperscalers* estadunidenses, ao compelir à Administração Pública Federal a contratação de serviços de provedores dos EUA, mediante contratos de longo prazo e investimentos públicos expressivos. Tal modelo cria demanda estável, estimula inovação doméstica e fortalece cadeias nacionais de valor em setores como computação em nuvem, semicondutores e IA. Ademais, se destacam o *CHIPS and Science Act* ou a Iniciativa *Stargate*, com previsão de investimentos massivos em P&D e produção de semicondutores e infraestruturas computacionais, com foco no reestabelecimento da capacidade de fabricação nacional e redução das dependências externas.

A **China** apresenta abordagem fortemente coordenada entre política industrial, regulação e governança estatal, além do desenvolvimento nacional de *hardware* e *software*. O apoio estratégico a arquiteturas como o RISC-V evidencia o uso do *open source* como instrumento pragmático de redução de dependências tecnológicas e fortalecimento da autonomia industrial, sob a égide de planos estratégicos como o *Internet Plus* e *Made in China 2025*. O primeiro foca na expansão da conectividade,

capacidade computacional e digitalização da administração pública, enquanto o segundo foca no desenvolvimento de uma cadeia interna de *design*, produção e empacotamento de *chips* e a formação de *clusters* tecnológicos nacionais, com a criação de nuvens soberanas, plataformas de dados públicos e privados e desenvolvimento de modelos e softwares, por meio de subsídios, incentivos fiscais e encomendas tecnológicas.

A experiência da **União Europeia** destaca-se pela liderança regulatória, destacando porém os enormes riscos de apostar na mera regulação para se construir a soberania digital. A EU soube inovar com instrumentos como o GDPR e o *AI Act*, que estabelecem padrões globais de proteção de dados e governança de IA. Porém tais instrumentos são necessários, mas não suficientes. O *European Chips Act*, surge como um esforço de reindustrialização e redução de dependências externas em semicondutores, porém sem escala suficiente para alterar a posição europeia nas cadeias globais de *hardware*. Ainda no âmbito regulatório, o *Cloud Sovereignty Framework* europeu define um *framework* de conformidade regulatória para avaliação de provedores de serviços de computação em nuvem interessados em participar de licitações públicas no espaço da União. Portanto, a experiência europeia revela os limites de uma abordagem predominantemente normativa e os riscos da ausência de políticas industriais robustas capazes de reduzir dependências infraestruturais.

A nota analisa experiencias de menor destaque. A experiência **suíça** é significativa ao desenvolver um LLM em *open source*, multilíngue por meio de uma colaboração entre instituições públicas de pesquisa. Dentre seus diferenciais estão o treinamento com grande conjunto de dados públicos. Entretanto, apresenta limitações, se restringindo a laboratórios governamentais ou grandes corporações tecnológicas. A **Finlândia** se destaca pela forte adesão ao uso de soluções *open source* autônomas por instituições públicas e privadas.

No contexto regional, o **Uruguai** demonstra que conectividade universal, investimento contínuo em infraestrutura nacional e adoção prioritária de *software livre* podem gerar ganhos significativos de autonomia tecnológica mesmo em países de menor escala. A **Índia**, por sua vez, ilustra o potencial das Infraestruturas Públicas Digitais, organizadas organicamente no plano de transformação digital *India Stack*, ao articular plataformas abertas, conectividade significativa e estímulo à inovação doméstica, permitindo expansão de serviços governamentais e florescimento de ecossistema privado vibrante. Entretanto, há críticas ao modelo, com forte concentração de poder institucional e informacional em poucas entidades estatais e paraestatais, que apresentam níveis de *accountability* limitados e risco de ampliação de vulnerabilidades sistêmicas.

6. PROPOSTA: A PILHA DIGITAL BRASILEIRA

A construção de um ecossistema nacional digitalmente soberano exige mais do que investimentos materiais ou ajustes regulatórios, necessitando de coordenação interinstitucional, fortalecimento científico, continuidade de políticas públicas, inserção internacional estratégica e capacidade de organizar recursos técnicos, humanos e financeiros. Neste sentido, a soberania digital brasileira é proposta a partir da noção de uma “pilha” digital nacional, entendida como arquitetura sociotécnica integrada, composta por seis camadas interconectadas: dados; algoritmos e modelos; infraestrutura computacional; infraestrutura de conectividade; recursos minerais e energéticos; e, transversalmente, capacitação e governança. Essa estrutura evidencia que a soberania digital não reside em um único nível da cadeia tecnológica, mas emerge do alinhamento entre capacidades técnicas, institucionais, materiais e humanas.

Na **camada de dados**, destaca-se a necessidade de plataformas de trocas de dados, chamadas de "bolsas de dados" e mecanismos de interoperabilidade que permitam o compartilhamento seguro e auditável de bases públicas e privadas, transformando dados em ativos estratégicos para pesquisa e inovação. Na **camada lógica,** o foco recai sobre o desenvolvimento e a adoção de modelos de IA nacionais, *software* livre e padrões abertos, assegurando auditabilidade, adaptabilidade e redução de dependências. A **camada de infraestrutura**, que se desdobra em duas subcamadas: *infraestrutura computacional* e *infraestrutura de conectividade*, sendo a primeira o nível material que viabiliza o treinamento, operação e escalonamento de modelos avançados, incluindo supercomputadores, *clusters* GPUT/TPU, *data centers* e nuvens sob jurisdição nacional. A segunda subcamada garante que dados, modelos e aplicações possam ser acessados e compartilhados de maneira não discriminatória, segura e eficiente.

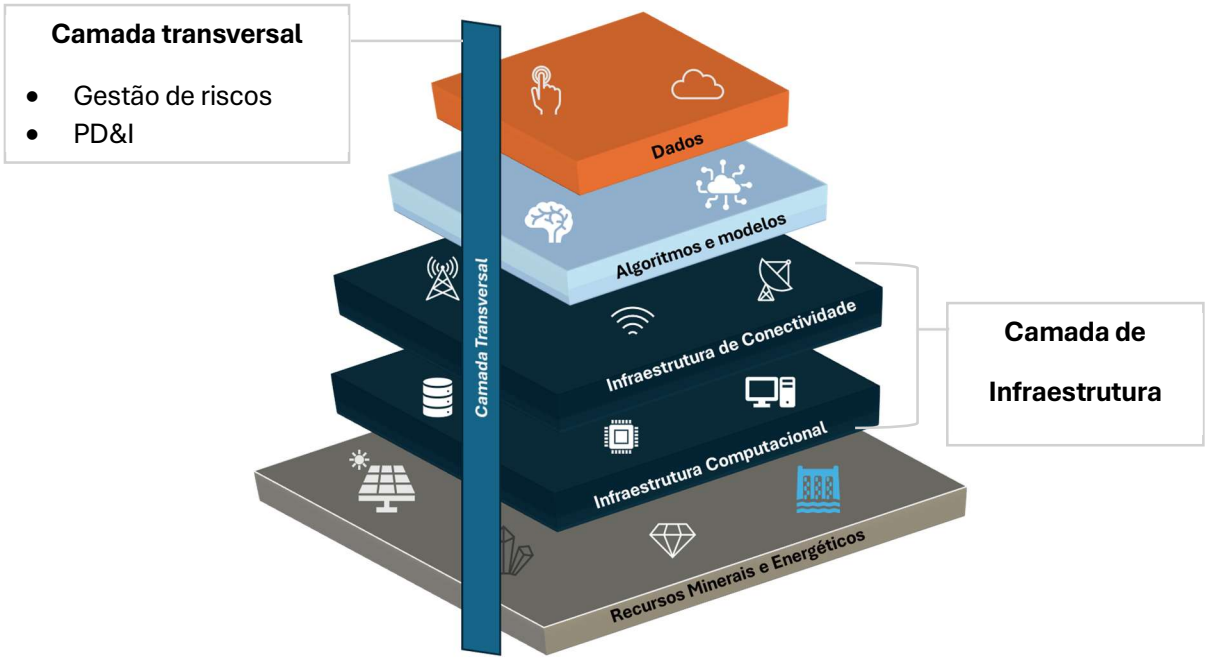

Figura 1. **Proposta de Pilha de IA Soberana Brasileira**

De forma **transversal**, a capacitação e treinamento de recursos humanos, a regulação de riscos e a cibersegurança, e a governança multissetorial permeiam toda a pilha, garantindo coordenação institucional, gestão de riscos, padronização técnica e alinhamento entre CT&I, indústria e Estado. Desta forma, a arquitetura apresentada demonstra que a consideração das demais dimensões da pilha digital brasileira é condição estruturante para o exercício pleno da soberana digital. Exemplos de excelência nacional, como a RNP, deveriam ser aprimorados para permitir a construção de uma pilha digital totalmente brasileira, reduzindo a dependência em computação em nuvem. E, no Brasil há atualmente pelo menos três frentes principais que poderiam ser melhor desenvolvidas e articuladas para promover essa construção: o **SINAPAD**, como provedor de serviços de supercomputação, formação de pessoas e desenvolvimento de produtos e serviços de processamento de alto desempenho, a iniciativa **Nuvem de Governo**, e o **REDATA**, ainda em discussão no Congresso.

7. RECOMENDAÇÕES ESTRATÉGICAS

As recomendações convergem para a necessidade de ação coordenada e de longo prazo. Dentre as principais recomendações seguem:

7.1. Estruturar uma arquitetura nacional de dados como pilar da Soberania Informacional

Recomenda-se a criação de uma Rede Nacional de Dados sob governança federada, capaz de viabilizar o compartilhamento seguro, auditável e juridicamente protegido de dados públicos e privados estratégicos. Essa rede deve integrar bases federais, estaduais e municipais por meio de padrões comuns de metadados, APIs, autenticação, cibersegurança e governança, assegurando interoperabilidade real e portabilidade informacional. A coordenação estratégica deve ocorrer no âmbito do CITDigital, centros de pesquisa e operadores públicos regionais.

Essa arquitetura deve ser concebida como infraestrutura essencial ao desenvolvimento de inteligência artificial nacional, permitindo o treinamento de modelos em bases de dados amplas, representativas e juridicamente seguras. Recomenda-se priorizar plataformas setoriais federadas (energia, petróleo e gás, clima, agronegócio, saúde e segurança pública) capazes de alimentar alianças estratégicas em IA, acompanhadas de mecanismos rigorosos de anonimização, cibersegurança controle de acesso e auditoria. É fundamental garantir a inclusão de dados regionais, multilíngues e de grupos historicamente sub-representados, assegurando que modelos nacionais sejam culturalmente contextualizados e socialmente inclusivos.

7.2. Alavancar centros de excelência e redes de pesquisa sob governança coordenada

Recomenda-se transformar o SINAPAD em infraestrutura pública estratégica plenamente operacional, atuando como prestador de serviços contínuos de computação cibersegura de alto desempenho, com ambientes padronizados, suporte técnico especializado, formação profissional e plataformas educacionais. Para isso, é indispensável assegurar financiamento previsível e de longo prazo, e parcerias estáveis, superando o modelo episódico de projetos isolados. As instituições devem ser integradas por meio de consórcios formais e redes temáticas nacionais, orientadas a missões estratégicas (energia, saúde, agroindústria, clima, segurança e cibersegurança). Essas redes devem compartilhar dados, infraestrutura computacional e ambientes seguros de desenvolvimento, favorecendo reprodutibilidade científica, escalabilidade e transferência tecnológica.

A participação da indústria deve ocorrer por meio de câmaras setoriais e comitês técnico-científicos, assegurando aderência às demandas produtivas e transformação de soluções em bens e serviços competitivos. No contexto brasileiro, o desenvolvimento autônomo de modelos fundacionais de fronteira em IA apresenta elevada complexidade técnica, financeira e institucional. Neste cenário, mostra-se mais racional e eficiente a constituição de alianças setoriais estratégicas, ancoradas em ativos tecnológicos nacionais já consolidados. Tal arranjo possibilitaria superar a fragmentação atual mediante articulação do SINAPAD, do futuro Sistema Nacional de Ciência, Tecnologia e Inovação em IA (SinIA), de padronização, e portfólio de missões estratégicas em saúde, clima, agricultura, petróleo e gás, e energia implementada por meio de alianças setoriais. Em suma, a criação de alianças estratégicas nos setores nos quais operam tais empresas, junto com universidades, e startups,

apresenta elevada viabilidade institucional e potencial impacto sistêmico, sobretudo na incorporação da IA, robótica avançada e manufatura de alta precisão. Desta forma, a coordenação estatal pode catalisar sinergias intersetoriais com efeitos econômicos, industriais e defensivos significativos.

7.3. Institucionalizar padrões nacionais de interoperabilidade e reprodutibilidade científica

Recomenda-se a definição e adoção obrigatória de padrões nacionais de interoperabilidade e cibersegurança, abrangendo dados, documentação, versionamento, *pipelines* de treinamento, governança de modelos e ambientes computacionais. Esses padrões devem ser formalizados por decreto e monitorados por instituições já existentes, como CITDigital, a SETAD/MCTI, CGI.br, ANPD e GSI, em articulação com o futuro sistema nacional de governança de IA (SinIA). A infraestrutura federada de dados e o SINAPAD devem oferecer ambientes padronizados com versões congeladas, ferramentas de auditoria automatizada e repositórios nacionais de código, modelos e documentação, inspirados em experiências como *Dataverse* e *HuggingFace Hub*. Essa abordagem é essencial para garantir transparência, confiabilidade, cibersegurança e cooperação científica em escala nacional, além de reduzir fricções institucionais e técnicas.

7.4. Mobilizar compras públicas para construir plataformas digitais soberanas

Recomenda-se o uso estratégico do poder de compra do Estado para estruturar um ecossistema nacional de plataformas profissionais *open source*, voltadas à comunicação institucional, colaboração, gestão documental e suporte à decisão. A administração pública deve priorizar soluções auditáveis, interoperáveis e hospedadas em infraestrutura sob jurisdição nacional, substituindo progressivamente softwares proprietários estrangeiros. Essas plataformas devem integrar modelos nacionais de IA, permitindo o desenvolvimento de assistentes e agentes inteligentes treinados em dados públicos e operando sob padrões éticos e de segurança definidos pelo próprio Estado. A infraestrutura existente (SINAPAD, SERPRO, nuvens nacionais, RNP) deve ser utilizada de forma mais estratégica e integrada.

Em especial, a RNP pode ser alavancada como núcleo estruturante de uma plataforma nacional de comunicação e colaboração profissional, baseada em tecnologias *open source* e IA desenvolvida no País, visto que o Sistema RNP provê conectividade avançada, software para colaboração profissional e serviços de nuvem para a rede acadêmica, demonstrando capacidade técnica e governança consolidada. A adoção em escala pela administração pública federal, com ampliação de data centers sob jurisdição nacional, permitiria reduzir dependência de plataformas estrangeiras e fortalecer a soberania digital. Ademais, recomenda-se que editais públicos incluam critérios explícitos de soberania digital: código aberto, portabilidade, documentação completa, conformidade com padrões nacionais e requisitos não negociáveis de cibersegurança.

7.5. Consolidar a CT&I como eixo estruturante da soberania digital

Recomenda-se fortalecer a articulação entre ENCTI 2024–2030, PBIA, SINAPAD, REDATA e Nova Indústria Brasil, evitando fragmentação institucional e sobreposição de incentivos. Para isso, é essencial designar uma instância executiva com mandato transversal, papel para o qual a SETAD/MCTI é o órgão mais indicado, sendo responsável por alinhar políticas, financiamento, prioridades e

implementação. Sua designação ocorreria em razão de seu escopo institucional, de suas competências legais e de sua posição estratégica na interface entre CT&I, transformação digital e políticas industriais. O fortalecimento desse papel permitiria conferir maior coerência sistêmica às ações em curso, reduzir redundâncias, maximizar sinergias entre programas e assegurar que investimentos públicos estejam efetivamente orientados aos objetivos de autonomia tecnológica e desenvolvimento nacional. Deste modo, recomenda-se também criar um programa transversal de soberania digital no âmbito do FNDCT, com foco em infraestrutura computacional, dados, modelos abertos e capacitação. Como alternativa politicamente viável, propõe-se a implementação inicial de programas setoriais de longo prazo em IA, articulados a missões estratégicas (energia, petróleo e gás, mudanças climáticas, agroindústria, saúde, finanças, telecomunicações, cibersegurança e defesa), funcionando como núcleos de consolidação progressiva da pilha digital soberana.

7.6. Desenvolver um *framework* brasileiro de soberania digital e compliance tecnológico

Recomenda-se a criação de um *Framework Brasileiro de Soberania Digital*, inspirado em experiências internacionais, mas ajustado ao ordenamento jurídico nacional. Esse *framework* deve articular três dimensões: soberania jurídica (jurisdição, proteção e segurança dos dados), soberania técnica (auditabilidade, interoperabilidade e abertura) e soberania operacional (controle de acesso, continuidade e resiliência). O *framework* deve incluir requisitos legais vinculantes, padrões técnicos mínimos, mecanismos de governança e um sistema escalonável de certificação e conformidade, com auditorias independentes. Tal estrutura permitirá reduzir vulnerabilidades sistêmicas, orientar contratações públicas privilegiando os serviços e produtos mais seguros, fortalecer a confiança institucional e alinhar tecnologia a valores constitucionais.

7.7. Integrar política digital aos setores estratégicos da economia

Recomenda-se estruturar alianças setoriais estratégicas em áreas como energia, petróleo e gás, mudanças climáticas, saúde, finanças, agroindústria, defesa, e cibersegurança utilizando esses setores como âncoras para o desenvolvimento de IA soberana. Essas alianças devem articular dados, infraestrutura, pesquisa e desenvolvimento, financiamento e demanda pública, por meio de consórcios envolvendo empresas líderes, universidades e centros de supercomputação. A política deve explorar vocações regionais e encadeamentos produtivos inter-regionais, integrando polos já estabelecidos como Rio de Janeiro, Campinas, São Paulo, Recife e Brasília em uma arquitetura federativa de inovação. Essa abordagem favorece escala, especialização territorial e redução de dependências tecnológicas. Ademais, é válida a exploração de novos encadeamentos produtivos inter-regionais, articulando polos regionais às demandas tecnológicas existentes, bem como discutir mecanismos para a interligação dos polos, construindo arquitetura federativa que capitalize as vocações regionais complementares.

7.8. Fortalecer cooperação internacional estratégica sem comprometer autonomia

Recomenda-se intensificar a atuação brasileira em quatro frentes junto a organismos internacionais, considerando a definição de padrões técnicos comuns (ISO, IEC, IEEE, IETF, W3C, ITU), em regimes multilaterais (ONU) e em arranjos regionais e plurilaterais (BRICS, Mercosul, UE–Mercosul), com

mecanismos de coordenação interna claros e estáveis entre MCTI, Itamaraty, CGI.br e agências reguladoras. A segunda frente é a necessidade parcerias internacionais para influenciar a definição de regimes internacionais que interessam as demais camadas da pilha, com base em princípios jurídicos, normas substantivas e mecanismos eficazes de resolução de controvérsias. A cooperação internacional deve priorizar padrões abertos, modelos de IA soberanos, cadeias de semicondutores, infraestrutura crítica e ciência aberta, sempre orientada por princípios de reciprocidade, transparência e proteção do interesse público nacional. A terceira frente é a cooperação científica internacional, permitindo ao Brasil reduzir dependência tecnológicas e ampliar sua capacidade de desenvolvimento de *software*, *hardware* e modelos próprios. A cooperação científica também fortalece boas práticas de ciência aberta, reprodutibilidade, auditoria e desenvolvimento responsável, criando ambientes regulatórios e institucionais alinhados a padrões globais de excelência científica. Por fim, a quarta frente é a cooperação comercial e industrial, com integração de cadeias produtivas internacionais, particularmente em setores estratégicos como semicondutores, equipamentos de telecomunicações, *hardware* avançado, serviços de nuvem, componentes críticos e modelos de IA. Tais arranjos permitirão atrair investimentos, desenvolver clusters industriais, participar de redes globais de inovação, diversificando demanda e oferta, e estabelecer acordo que reduzam vulnerabilidades materiais na camada de recursos minerais e energéticos e os riscos de interdependências instrumentalizadas.

8. CONSIDERAÇÕES FINAIS

A soberania digital brasileira não é um estado fixo a ser alcançado, mas um processo contínuo e multidimensional que exige visão estratégica de longo prazo, coordenação intergovernamental e compromisso com o desenvolvimento científico e industrial. O Brasil dispõe de ativos relevantes, base legislativa avançada, ecossistema acadêmico competitivo e infraestrutura de supercomputação em expansão, mas enfrenta vulnerabilidades persistentes, como dependência quase total de hardware e software estrangeiros, fragmentação institucional e baixa cultura tecnológica soberana nos órgãos públicos. A experiência internacional demonstra que não existe modelo único a ser replicado: cada país combinou regulação, política industrial, compras públicas e governança de forma própria, cabendo ao Brasil construir sua estratégia adaptada às condições locais.

Para avançar nessa agenda, são necessárias ações em múltiplos eixos: harmonização regulatória com marco claro para infraestruturas críticas e IA de alto risco; governança multissetorial integrada pelo CITDigital; mobilização das compras públicas como instrumento de política industrial; criação de um *framework* nacional de *compliance* para nuvem e IA; e investimento em modelos abertos, bibliotecas nacionais, semicondutores e plataformas federadas de dados. A sustentabilidade dessas políticas depende de mecanismos permanentes de financiamento, implementação sequenciada em fases e monitoramento contínuo por meio de um Conjunto de Indicadores de Soberania Digital, não como isolamento tecnológico, mas como autonomia estratégica para escolher, produzir, auditar e governar tecnologias essenciais ao interesse nacional.

Para subsidiar essa agenda de longo prazo, estudos futuros devem se concentrar em três frentes prioritárias: o desenvolvimento de métricas e indicadores capazes de mensurar dimensões como autonomia informacional, resiliência cibernética e dependência de fornecedores estrangeiros; a análise comparada aprofundada de modelos de governança digital adotados por países como EUA, China, Índia, Uruguai e Suíça, com foco em seus mecanismos de coordenação e estabilidade institucional; e o

mapeamento sistemático dos fóruns internacionais de padronização e regulação tecnológica, ISO, ITU-T, IETF, ONU, BRICS e G20, identificando agendas, atores dominantes e oportunidades concretas de influência brasileira. Esses estudos fornecerão a base empírica e institucional para que o Brasil exerça controle legítimo e democrático sobre as infraestruturas que sustentarão seu futuro tecnológico.