

Contribuição Conjunta à Tomada de
Subsídios para eixo de infraestrutura
e conectividade da **Política Nacional
de Data Centers**



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife



LAPIN
LABORATÓRIO DE POLÍTICAS
PÚBLICAS E INTERNET

FICHA TÉCNICA

SOBRE NÓS

O IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife é uma organização sem fins lucrativos dedicada à pesquisa, capacitação, comunicação e impacto político acerca das tecnologias. Concentra-se em debates multissetoriais, direitos humanos, diversidade e perspectivas regionais no ambiente digital/tecnológico. O instituto considera a sociedade civil organizada um motor fundamental do diálogo político, intrinsecamente ligado ao uso ativo da tecnologia.

O Laboratório de Políticas Públicas e Internet - LAPIN é um centro independente de pesquisa e ação sediado em Brasília, Brasil, focado em políticas digitais e regulação tecnológica. Ele investiga impactos sociais, econômicos, éticos e jurídicos, enquanto promove inclusão social, alfabetização digital e soluções inovadoras para governança digital.

AUTORES

André Fernandes - Diretor e Fundador do IP.rec

Helton Leyendecker - Pesquisador do IP.rec

Anicely Santos - Pesquisadora do IP.rec

Camila Cristina da Silva - Coordenadora do GT IA do LAPIN

Cynthia Picolo Gonzaga de Azevedo - Diretora Executiva do LAPIN

Isabelle Alves Moreira de Oliveira - Pesquisadora do LAPIN

Marcelo Aparecido de Faria Junior - Pesquisador do LAPIN

Maria Luiza Duarte Sá - Pesquisadora do LAPIN

CONTATOS

IP.rec

andrefernandes@ip.rec.br

heltonleyendecker@ip.rec.br

LAPIN

cynthia.picolo@lapin.org.br

felipe@lapin.org.br



INTRODUÇÃO

Este documento reúne as contribuições conjuntas do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) e do Laboratório de Políticas de Internet (Lapin) para a Tomada de Subsídios conduzida pelo Ministério das Comunicações. As recomendações apresentadas têm como objetivo orientar a formulação de uma Política Nacional de Data Centers comprometida com a justiça socioambiental, a soberania digital e o desenvolvimento sustentável do Brasil.

As proposições estão organizadas em tópicos temáticos e foram elaboradas a partir de análises jurídicas, técnicas e socioambientais. O foco é assegurar que os data centers, enquanto infraestrutura crítica para a economia digital e para a soberania nacional, não sejam apenas indutores de competitividade fiscal, mas também instrumentos de fortalecimento regional, inovação responsável e proteção de direitos fundamentais.

O documento sintetiza os pontos centrais que consideramos indispensáveis para uma política pública robusta: princípios estratégicos, objetivos de longo prazo, diretrizes regulatórias, mecanismos de transparência e participação social, critérios de localização e estratégias de estímulo ao desenvolvimento regional.

RECOMENDAÇÕES:

1. O Redata deve ser guiado por três princípios estratégicos: justiça socioambiental, soberania digital e sustentabilidade. Justiça Socioambiental significa integrar meio ambiente e sociedade, assegurando que todos os grupos tenham igual direito de acesso aos recursos naturais. É o alinhamento entre interesse econômico e isonomia, garantindo que os benefícios e ônus socioambientais da política pública sejam distribuídos de forma equitativa, com a participação ativa das comunidades nas decisões que afetam seus territórios. A soberania digital deve priorizar o interesse público nacional, e não apenas interesses privados.

Os recursos naturais do Brasil são ativos estratégicos e não podem ser usados como moeda para o lucro de empresas estrangeiras e fundos internacionais. A sustentabilidade deve ser um princípio orientador, indo além de discursos corporativos de "práticas sustentáveis" e compromissos voluntários, com obrigações legais de indicadores claros de impacto ambiental e social.

2. É essencial adotar uma abordagem que equilibre crescimento tecnológico e justiça socioambiental: um marco regulatório robusto, com lei específica para data centers e suas implicações ambientais, além de normas obrigatórias de transparência sobre relatórios periódicos detalhados em português. Também é necessário definir métricas holísticas padrão para monitorar o consumo de recursos, mecanismos independentes de verificação e certificação ambiental auditável e baseada em critérios objetivos. Fomentar pesquisas e projetos para promover uma transição energética justa e eficiente, exigindo o uso de fontes renováveis adicionais, regulamentando certificados de energia renovável e financiando a computação sustentável. Outro ponto fundamental é garantir a sustentabilidade hídrica, com exigências de reposição de água e reporte obrigatório. A política também deve consolidar uma governança participativa e assegurar contrapartidas sociais e ambientais como condição para benefícios fiscais.

3. Os principais desafios incluem o alto consumo de energia e água, intensificado pela expansão da IA; os impactos socioambientais da chamada "energia limpa" e o risco de *greenwashing*; a falta de transparência e padronização nos relatórios de prestação de contas; a dependência da mineração de minerais críticos; a geração excessiva de resíduos eletrônicos; e a ausência de um marco regulatório específico sobre suas implicações socioambientais. Para enfrentá-los de forma eficaz: (i) definir métricas padronizadas de consumo, emissões e eficiência; (ii) garantir relatórios transparentes, públicos, auditáveis e acessíveis em português; (iii) garantir participação e consulta prévia às comunidades afetadas; (iv) condicionar incentivos fiscais e financiamentos ao cumprimento de metas ambientais verificáveis; (v) exigir a redução real do uso de recursos; (vi) assegurar a

rastreabilidade da cadeia mineral; e (vii) estabelecer diretrizes para a gestão responsável de resíduos eletrônicos.

4. A Política Nacional de Data Centers deve se integrar ao Plano Brasileiro de Inteligência Artificial (PBIA). Embora o PBIA reconheça data centers como infraestrutura crítica para IA (Eixo 1), sua menção ao baixo impacto ambiental é vaga. Existem lacunas: fala-se em eficiência energética e uso responsável da água, mas não há definição de métricas como PUE (eficiência energética), WUE (eficiência hídrica), nem critérios claros de localização ou exigências sobre energia renovável adicional. O PBIA já prevê o investimento “Pró-Infra IA Sustentável” (Eixo 1) para fomentar infraestrutura energética sustentável, e menciona (Eixo 4) a criação de data centers “verdes” de alta capacidade, alimentados por renováveis e com uso hídrico otimizado, mas não define como e o que seria isso. Esses pontos precisam ser harmonizados concretamente entre o REDATA e o PBIA, transformando conceitos abertos em obrigações verificáveis e vinculando incentivos públicos a contrapartidas socioambientais.

5. O atual arcabouço legal e regulatório marca um cenário de insegurança jurídica, pois não existe lei específica para que o setor de data centers se desenvolva com responsabilidade e em alinhamento à justiça socioambiental. As regras atuais de licenciamento ambiental são insuficientes para avaliarem o nível de impacto socioambiental de grandes projetos de data centers, pois estão no campo da discricionariedade normativa e administrativa de cada município e estado. Assim, são liberadas as instalações por meio de enquadramentos ambientais incompatíveis e desproporcionais, como um data center ser equiparado a um “parque de vaquejada”. Isso é evidenciado no caso da licença ambiental concedida ao data center do Tiktok, em Caucaia, no Ceará, em que o projeto foi considerado de “baixo impacto ambiental”, com dispensa de estudos mais detalhados, mesmo sendo a demanda energética anual equivalente ao de 2,2 milhões de brasileiros, como a reportagem investigativa do Intercept Brasil revelou. Isso expõe a flexibilização excessiva e a ausência de critérios técnicos uniformes. Deve-se fortalecer, no

mínimo, resoluções nacionais do Conselho Nacional do Meio Ambiente (CONAMA), por exemplo, que tratem especificamente de regras e orientações do licenciamento ambiental dos data centers. Normas desse tipo fortaleceriam tanto a segurança jurídica para empresas sérias quanto a proteção socioambiental, evitando o aprofundamento de desigualdades.

6. Temas regulatórios devem ser priorizados garantindo equilíbrio entre direitos, sustentabilidade e crescimento econômico. Em primeiro lugar, a justiça socioambiental, essencial para assegurar que os benefícios e os custos do desenvolvimento sejam distribuídos equitativamente. Em segundo, a proteção aos povos originários e comunidades tradicionais, respeitando processos de consulta prévia, tradições e direitos constitucionais, especialmente pelas pressões sobre recursos naturais. Em terceiro lugar, o impacto das fontes renováveis, garantindo que a transição energética seja justa, priorizando substituição ao invés de acumulação. Em quarto, a soberania digital, vinculando incentivos à inovação e à autonomia tecnológica nacional. Por fim, o desenvolvimento econômico, que deve ser condicionado a compromissos socioambientais vinculantes, evitando políticas que priorizem apenas a competitividade fiscal.

7. A gestão de data centers deve estar vinculada a conselhos locais de gestão ambiental e social, com composição multissetorial, incluindo comunidade local, com representação específica para comunidades tradicionais. O governo federal deve estabelecer normas unificadas e obrigatórias de transparência, padronizando indicadores, métricas e metodologias de quantificação do impacto ambiental. Os dados devem ser publicados em plataforma única para registro histórico e de acesso público, com periodicidade definida. As empresas devem reportar dados ambientais que incluam a diferenciação clara entre emissões de carbono evitadas, compensadas e remanescentes, origem e aquisições via contratos de energia renovável, balanços hídricos completos e rastreabilidade da cadeia mineral. Também devem existir canais permanentes de participação social, com consultas periódicas e instâncias de deliberação popular.

8. Data centers não devem ser instalados em territórios indígenas, quilombolas ou outras comunidades tradicionais que dependem do território para sua subsistência, mesmo aqueles ainda não demarcados. Também deve ser vedada a instalação em áreas com histórico ou risco de escassez hídrica ou energética. Ainda, deve-se proibir a construção em áreas adjacentes a reservas naturais, unidades de conservação, áreas de preservação permanente, regiões agrícolas, áreas densamente povoadas ou sujeitas a enchentes, calor extremo e deslizamentos, que comprometem a operação e a segurança. As instalações também não deverão ocorrer em locais onde o consumo energético pressione e/ou comprometa o fornecimento de energia às populações e comunidades.

9. Devem ser estabelecidas zonas de interesse, desde que definidas com base em critérios regulatórios socioambientais rigorosos, e não apenas técnicos ou de conectividade. Isso porque data centers de grande porte demandam uso contínuo e intensivo de energia e água, gerando pressões sobre infraestruturas locais de distribuição, podendo competir com comunidades que muitas vezes já enfrentam limitações no acesso a esses recursos básicos. Sem delimitação territorial clara, essas infraestruturas tenderão a se instalar em localidades com menor resistência institucional, menor custo de terra e proximidade de recursos naturais abundantes – ecossistemas sensíveis e/ou territórios já ocupados por comunidades. Por serem estruturas físicas de grande escala, sua instalação exige avaliação criteriosa do uso do solo, para mitigar impactos sobre o equilíbrio ambiental local, áreas de proteção ambiental, fauna e flora nativa. Zonas de interesse devem ser definidas a partir de critérios que assegurem, primeiramente, equilíbrio socioambiental. Isso envolve considerar a disponibilidade de fontes renováveis de energia e os efeitos de sua geração, bem como as estimativas de consumo hídrico e sua relação com corpos d'água ou aquíferos locais. Também é necessário avaliar a compatibilidade territorial, evitando sobreposição com comunidades já instaladas, atividades produtivas ou áreas de preservação ambiental. Além disso, a regulação precisa garantir transparência e mecanismos de participação social.

10. Para estimular a instalação de data centers em regiões menos desenvolvidas, a política deve combinar incentivos fiscais e linhas de crédito condicionados a investimentos em infraestrutura pública, energia renovável e conectividade comunitária. Esses empreendimentos podem ser atraídos pela integração com vocações regionais, como o aproveitamento do excedente de energia solar no Nordeste, da força eólica no litoral ou de climas favoráveis ao resfriamento natural e pela segurança hídrica que evite competição com populações locais. Essencial garantir que a fixação de valor permaneça no território, por meio de parcerias obrigatórias com universidades e centros de pesquisa e formação de mão de obra, bem como cotas de contratação de fornecedores locais. A política pode ainda estimular que data centers expandam redes de transmissão elétrica e de fibra ótica compartilhadas com a população e aproveitem o calor dissipado em atividades econômicas locais.

11. Condicionar licenças e incentivos a: (i) planos locacionais que evitem áreas com estresse hídrico e priorizem regiões com excedente de energia renovável; (ii) métricas e reporte público contínuo (PUE, WUE, EUI, fator de carbono) em painéis abertos; (iii) gestão de demanda (tarifas horárias, contratos de resposta, armazenamento, geração no local) sem subsídio cruzada; (iv) reuso de água/efluentes e reaproveitamento de calor; (v) avaliação ambiental e social cumulativa com participação significativa de comunidades; (vi) acordos de benefícios comunitários; (vii) “não concorrência” com serviços essenciais em situações de estiagem/calamidade; (viii) sinal locacional nas redes (energia/backhaul) e obrigações de transparência. Garantir que sejam usados dashboards públicos em tempo real e vinculação a políticas industriais que promovam inovação local e cadeias circulares, evitando dependência exclusiva de hyperscalers.

12. Exigir segurança e privacidade-by-design: criptografia em repouso/trânsito, segregação de redes, zero-trust, gestão de chaves no país, hardening e SBOM. Obrigar DPIA/LIA e minimização de dados, com auditorias



independentes e relatórios de incidentes a autoridades competentes; certificações setoriais e testes de resiliência. Para soberania: dados e workloads críticos com guarda e processamento sob jurisdição brasileira ou com salvaguardas equivalentes; transparência sobre fluxos transfronteiriços; cadeias de suprimento auditáveis; proibir backdoors; alinhar com LGPD/ANPD e políticas nacionais de cibersegurança, com coordenação interministerial. Promoção governança participativa (sociedade civil e academia) e requisitos de diversificação de fornecedores, fortalecendo resiliência geopolítica e interoperabilidade auditável.



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife



LAPIN
LABORATÓRIO DE POLÍTICAS
PÚBLICAS E INTERNET