Soberania digital, infraestruturas críticas e geoeconomia da inteligência artificial

Raymundo Campos Neto

1. Introdução: quando a infraestrutura digital se converte em poder público indireto

A digitalização contemporânea deslocou o centro material da soberania. Durante boa parte da modernidade jurídica, a pergunta fundamental do Estado era territorial: quem exerce autoridade sobre pessoas, bens, recursos naturais e instituições situadas em determinado espaço? Na economia digital, essa pergunta permanece necessária, mas se tornou insuficiente. A administração pública, o mercado financeiro, a segurança, a saúde, a justiça, a educação, a tributação, a comunicação social e a própria deliberação democrática passam a depender de camadas técnicas que frequentemente não se encontram sob controle jurídico, econômico ou operacional do Estado que delas necessita. A soberania deixa de ser apenas uma categoria de fronteiras; converte-se também em uma categoria de infraestrutura.

O episódio recente em torno da restrição de acesso a modelos avançados de inteligência artificial da Anthropic, noticiado no Brasil a partir de entrevista com Francesca Bria, oferece um ponto de partida emblemático. A imagem do "botão de desligar" sintetiza uma mudança de época: o acesso a capacidades computacionais essenciais pode ser condicionado por decisões administrativas de outro Estado, por regimes de sanções, por controles de exportação, por cláusulas contratuais assimétricas ou por arquiteturas técnicas que impedem substituição tempestiva. Essa ocorrência não deve ser lida como anedota isolada, mas como sintoma de uma geoeconomia da IA em que infraestrutura, jurisdição e poder de mercado se combinam. [1]

O problema jurídico não consiste em negar que Estados possam proteger interesses essenciais de segurança. O direito internacional sempre admitiu, em graus diversos, margens de autopreservação estatal. O ponto decisivo é outro: quando a infraestrutura digital global se organiza em redes concentradas, controladas por poucas empresas submetidas a poucas jurisdições, a invocação de segurança nacional por um Estado pode produzir efeitos funcionais equivalentes a sanções globais. O que era apresentado como serviço privado passa a operar como mecanismo de coerção pública indireta. A nuvem deixa de ser mera hospedagem; modelos fundacionais deixam de ser meras ferramentas; sistemas de pagamento deixam de ser meros instrumentos financeiros. Todos se transformam em pontos de estrangulamento de cadeias econômicas, administrativas e democráticas.

A soberania, nesse contexto, precisa ser reconstruída sem nostalgia e sem ingenuidade. Não se trata de regressar a uma soberania absoluta, fechada e impermeável, que a própria história do direito internacional demonstra nunca ter existido de forma pura. A literatura clássica já descreveu a soberania como instituição atravessada por compromissos, ficções, assimetrias e hipocrisias organizadas. [2] Tampouco se pode ignorar que a interdependência econômica sempre produziu ganhos de escala, eficiência e inovação. O desafio é qualificar juridicamente a dependência. Há dependências ordinárias, próprias de uma economia aberta; há, porém, dependências críticas que tornam um Estado incapaz de assegurar a continuidade de funções públicas essenciais sem autorização, tolerância ou estabilidade política de terceiros.

A hipótese central deste artigo é que soberania digital deve ser compreendida como capacidade institucional de governar dependências digitais críticas. Ela não equivale à fabricação nacional de todos os componentes tecnológicos, nem à expulsão de fornecedores estrangeiros. Equivale, antes, à preservação de um mínimo soberano: dados estratégicos sob governança jurídica efetiva; sistemas públicos essenciais com continuidade operacional; pagamentos e identidade digitais controláveis democraticamente; contratos de nuvem e IA com reversibilidade; padrões abertos; capacidades computacionais públicas ou compartilhadas; mecanismos de auditoria; e política industrial orientada à aprendizagem, à competição e ao valor público. Em linguagem econômica, trata-se de reduzir vulnerabilidades de hold-up, lock-in e apropriação externa de rendas; em linguagem jurídica, trata-se de proteger a autodeterminação democrática diante de infraestruturas privadas transnacionais.

A relevância do tema é transversal. No direito internacional econômico, a soberania digital tensiona comércio de serviços, fluxos de dados, compras governamentais, segurança nacional e concorrência. Na economia, reabre o debate sobre política industrial, inovação, bens públicos, dependência tecnológica e captura de valor. No direito constitucional e administrativo, questiona a capacidade do Estado de cumprir direitos fundamentais quando seus instrumentos de execução dependem de plataformas que ele não controla. Na teoria democrática, coloca a pergunta sobre quem governa a esfera pública quando a mediação comunicativa é organizada por infraestruturas algorítmicas privadas. Assim, falar em soberania digital é falar simultaneamente de jurisdição, desenvolvimento, competição, segurança, direitos fundamentais e democracia.

2. Método, delimitação e tese

O método adotado é bibliográfico-documental, com análise jurídico-econômica. A pesquisa mobiliza literatura sobre soberania, interdependência complexa, economia política internacional, regulação da informação, economia da inovação, infraestrutura pública digital e governança de IA. Também examina documentos normativos e institucionais recentes, como o AI Act europeu, o Digital Markets Act, o Data Act, o Cloud Act norte-americano, instrumentos de sanções contra o Tribunal Penal Internacional, materiais da OMC sobre exceções de segurança e comércio digital, documentos do G20 sobre infraestrutura pública digital, documentos da UNCTAD sobre fluxos de dados e relatórios do Banco Central do Brasil sobre o Pix. [3]

A delimitação é intencionalmente transversal. O artigo não pretende resolver tecnicamente a engenharia de uma nuvem soberana, nem desenhar arquitetura de semicondutores ou modelos fundacionais. Seu objetivo é construir uma moldura jurídico-econômica apta a orientar políticas públicas, contratos, regulação e cooperação internacional. A tese defendida é que a soberania digital democrática depende de três movimentos simultâneos: primeiro, identificar camadas críticas do stack digital; segundo, reduzir assimetrias estruturais de dependência por meio de padrões abertos, compras públicas, interoperabilidade e capacidades próprias; terceiro, submeter tais capacidades a garantias democráticas, para que a cura contra a dependência privada estrangeira não produza uma patologia de vigilância estatal ou autoritarismo tecnológico.

A categoria “stack digital” é utilizada em sentido analítico: refere-se às camadas técnicas, econômicas e jurídicas que tornam possível a vida digital. Inclui matérias-primas, energia, semicondutores, data centers, nuvem, conectividade, sistemas operacionais, bases de

dados, modelos de IA, aplicações, identidade digital, pagamentos, cibersegurança, padrões e regimes contratuais. A literatura de Benjamin Bratton propõe uma leitura do stack como arquitetura planetária de governança; Lawrence Lessig, por sua vez, já havia demonstrado que o código atua como modalidade regulatória. [4] A contribuição deste artigo é aproximar essas intuições de uma agenda de direito internacional econômico e de desenvolvimento.

A investigação parte de uma premissa de realismo institucional: mercados digitais não são espaços naturais de espontaneidade técnica, mas arranjos jurídicos estruturados por propriedade intelectual, contratos, investimentos públicos, subsídios, padrões, infraestrutura energética, regimes de responsabilidade e políticas de segurança. A questão, portanto, não é se o Estado deve ou não intervir. Ele já intervém ao criar direitos de exclusividade, comprar tecnologia, reconhecer assinaturas digitais, estabelecer padrões de interoperabilidade, permitir concentração, proteger segredos industriais e organizar redes de pagamento. A questão correta é qual intervenção produz autonomia, competição, direitos e desenvolvimento, e qual intervenção aprofunda dependência.

3. Soberania digital: entre jurisdição, capacidade e valor

Soberania digital não deve ser definida como posse integral de tecnologia. A posse é uma dimensão relevante, mas insuficiente. Um Estado pode possuir determinados ativos e, ainda assim, ser incapaz de operá-los, auditá-los, atualizá-los ou protegê-los. De modo inverso, pode não fabricar todos os componentes e, mesmo assim, preservar autonomia se dispuser de governança contratual, redundância, padrões abertos, chaves criptográficas, jurisdição efetiva, capacidade técnica e opções reais de substituição. A soberania digital é, portanto, menos uma ontologia da propriedade e mais uma teoria da capacidade institucional.

Essa capacidade possui ao menos quatro dimensões. A primeira é decisória: a comunidade política deve poder decidir os fins legítimos de sua infraestrutura digital, em conformidade com Constituição, direitos fundamentais e deliberação democrática. A segunda é operacional: serviços essenciais não podem ser descontinuados por decisão unilateral de fornecedor, sanção estrangeira ou falha sistêmica sem contingência. A terceira é econômica: os fluxos de valor gerados por dados, pagamentos, aplicações e inovação não podem ser integralmente extraídos por plataformas externas sem encadeamentos produtivos domésticos. A quarta é epistêmica: o Estado e a sociedade precisam compreender, auditar e contestar sistemas que classificam pessoas, distribuem oportunidades, priorizam informações e automatizam decisões.

A soberania digital também difere de localização compulsória indiscriminada de dados. Localizar dados no território nacional pode ser importante em alguns casos, mas não resolve, por si só, a dependência. Se os dados estão fisicamente no país, mas sob administração técnica de fornecedor sujeito a ordens extraterritoriais, com chaves sob controle externo e sem capacidade local de migração, a soberania é apenas aparente. A questão central é a governança efetiva: quem controla o acesso, quem administra chaves, quem audita, quem responde por incidentes, quem decide continuidade e quem captura o valor produzido. [5]

A economia política internacional ajuda a compreender essa mutação. Keohane e Nye demonstraram que a interdependência não distribui poder de modo simétrico; Farrell e Newman avançaram ao demonstrar como redes globais podem ser armadas por Estados

que controlam nós centrais. [6] A economia digital radicaliza essa hipótese porque muitos nós centrais não são apenas logísticos ou financeiros, mas cognitivos: nuvens, modelos de IA, lojas de aplicativos, sistemas de identidade, APIs, sistemas de anúncios, trilhos de pagamento e ambientes de desenvolvimento. Quem controla esses nós não controla apenas fluxos; controla possibilidades.

Susan Strange já havia advertido que a difusão do poder na economia mundial não significava desaparecimento do poder, mas deslocamento de suas formas. [7] O ponto se torna mais agudo quando infraestruturas privadas passam a condicionar a execução de tarefas públicas. Um tribunal, uma secretaria de saúde, uma autoridade tributária, um banco central ou uma universidade podem continuar juridicamente soberanos, mas operacionalmente dependentes de contratos que os expõem a jurisdições estrangeiras e padrões técnicos opacos. A soberania formal permanece; a soberania funcional se estreita.

Essa distinção entre formalidade e funcionalidade é essencial. A soberania clássica preserva o direito de editar normas; a soberania digital exige capacidade de fazer com que tais normas sejam efetivas sobre sistemas técnicos. Um país pode aprovar lei de proteção de dados, mas será pouco efetivo se não conseguir auditar fluxos, exigir portabilidade, impor sanções a agentes transnacionais ou oferecer alternativas públicas. Pode aprovar política de IA ética, mas será vulnerável se os modelos críticos forem inacessíveis, fechados, hospedados fora de sua jurisdição e incorporados a processos administrativos sem explicabilidade. Pode regular pagamentos, mas será dependente se a infraestrutura de liquidação, autenticação ou carteira digital estiver subordinada a oligopólios estrangeiros.

4. Dados, nuvem, IA, chips e pagamentos: a nova materialidade da soberania

A economia digital costuma ser descrita como imaterial. Essa descrição é enganosa. A IA depende de energia, data centers, semicondutores, cabos submarinos, minerais críticos, engenheiros, bases de dados, modelos matemáticos, direitos de propriedade intelectual, sistemas de refrigeração, contratos de nuvem e regimes de exportação. A nuvem é uma metáfora leve para uma infraestrutura pesada. A inteligência artificial é uma metáfora cognitiva para um complexo industrial intensivo em capital, energia, dados e computação. A soberania digital começa quando se abandona a ilusão de imaterialidade e se reconhece a base física, jurídica e econômica do digital.

A UNCTAD tem insistido que os fluxos de dados se tornaram recursos estratégicos para criação de valor, mas sua captura é profundamente desigual. [8] Países em desenvolvimento podem gerar dados, usuários e mercados sem capturar valor proporcional em inteligência, propriedade, tributação, infraestrutura e inovação. Essa assimetria reproduz, em nova linguagem, antigos padrões centro-periferia: a periferia fornece matéria-prima informacional; o centro transforma dados em modelos, serviços, propriedade intelectual, renda monopolista e poder regulatório de fato. O dado, nesse sentido, não é “o novo petróleo” apenas por seu valor econômico; é também matéria-prima de capacidade estatal, vantagem competitiva e assimetria geopolítica.

Os semicondutores e a capacidade computacional ocupam papel análogo ao de insumos estratégicos em revoluções industriais anteriores. A literatura sobre tecnologias de propósito geral mostra que certas inovações não criam apenas novos setores; reorganizam todos os setores. [9] A IA fundacional, ao se integrar a saúde, justiça, educação, defesa,

finanças e administração pública, aproxima-se dessa categoria. Quem controla o acesso ao poder computacional e aos modelos de fronteira controla, em parte, o ritmo de difusão da produtividade, o custo de entrada de competidores e a autonomia de Estados na implementação de políticas públicas.

A nuvem, por sua vez, converte-se em camada de dependência transversal. Ela hospeda bancos de dados públicos, sistemas judiciais, prontuários, ferramentas de colaboração, aplicações fiscais, serviços de segurança, sistemas educacionais e ambientes de IA. A dependência de nuvem é particularmente sensível porque combina lock-in técnico, custos de migração, contratos de longa duração, escassez de competências internas e assimetria de negociação. A questão não é demonizar provedores globais, cuja escala produziu ganhos relevantes de segurança, disponibilidade e inovação. O problema é tratar essa dependência como se fosse apenas compra ordinária de serviço, quando ela define a continuidade do Estado.

Os sistemas de pagamento revelam de modo claro a dimensão pública da infraestrutura digital. O Pix demonstra que uma infraestrutura estatal, interoperável, gratuita para pessoas físicas em muitos usos, regulada pelo Banco Central e aberta a participantes privados pode reorganizar mercados, reduzir custos de transação, aumentar inclusão e criar trilhos nacionais de valor. [10] A experiência brasileira é relevante porque mostra uma terceira via entre monopólio estatal fechado e dependência integral de plataformas privadas estrangeiras. O Estado não precisa operar todos os serviços finais; pode construir a camada comum sobre a qual agentes privados competem.

Essa camada comum é precisamente o que a literatura recente chama de infraestrutura pública digital. O Banco Mundial, a OCDE e o G20 convergem ao descrever DPI como sistemas digitais compartilhados, reutilizáveis, interoperáveis, seguros e orientados a permitir serviços públicos e privados em escala. [11] O ponto jurídico essencial é que tais infraestruturas não são apenas projetos tecnológicos; são instituições. Elas distribuem poder, custos, oportunidades e riscos. Por isso, precisam de governança, accountability, controle social, segurança cibernética, proteção de dados e regras concorrenciais.

5. Interdependência armada e extraterritorialidade: o direito internacional diante do “botão de desligar”

A soberania digital torna-se urgente quando a interdependência deixa de ser apenas condição de cooperação e se torna instrumento de coerção. A expressão “weaponized interdependence” descreve a capacidade de Estados situados no centro de redes globais de monitorar ou bloquear fluxos que passam por nós sob sua influência. [12] No ambiente digital, essa capacidade se manifesta em pelo menos quatro instrumentos: sanções financeiras e tecnológicas; controles de exportação; ordens de acesso a dados; e pressão sobre empresas que operam infraestrutura crítica mundial.

O Cloud Act norte-americano é exemplo de como a jurisdição sobre empresas pode projetar efeitos para dados armazenados fora do território. [13] A preocupação europeia com soberania de dados não decorre apenas de abstrata rivalidade econômica, mas de um conflito real entre localização física, controle corporativo e alcance jurídico. Quando uma empresa submetida à jurisdição de um Estado opera infraestrutura crítica em outro, surge uma zona cinzenta: o cliente público local pode acreditar que seus dados estão protegidos pela territorialidade do armazenamento, enquanto o fornecedor permanece sujeito a

ordens estrangeiras. A soberania, nesse caso, depende menos do lugar do servidor e mais da arquitetura de controle jurídico-técnico.

As sanções contra o Tribunal Penal Internacional, especialmente seus efeitos sobre contas, serviços e e-mails vinculados a autoridades do Tribunal, evidenciam o potencial de infraestruturas privadas globais como instrumentos de política externa. [14] O problema ultrapassa o caso concreto e atinge a arquitetura institucional do direito internacional. Se tribunais internacionais, organizações humanitárias ou entidades multilaterais dependem de serviços digitais sujeitos a sanções unilaterais de um Estado não parte ou adversário político, a independência funcional dessas instituições fica vulnerável. O direito internacional, que historicamente protegeu sedes, arquivos, imunidades e comunicações, precisa atualizar essa proteção para camadas digitais.

Controles de exportação sobre chips e modelos de IA representam outra dimensão. Estados têm razões legítimas para impedir usos militares, cibernéticos ou repressivos de tecnologias sensíveis. Contudo, a expansão de controles para acesso a modelos em nuvem, nacionalidade de usuários ou capacidades abstratas de software cria desafios jurídicos inéditos. Quando o objeto controlado é um serviço cognitivo global, a fronteira entre exportação, prestação transfronteiriça de serviços, transferência de tecnologia e controle de informação torna-se instável. A literatura recente sobre controles de exportação em IA destaca riscos de eficácia limitada, incentivos à substituição adversarial e tensões com obrigações comerciais multilaterais. [15]

No plano da OMC, as exceções de segurança previstas no GATT e no GATS não podem ser lidas como carta branca ilimitada. O relatório Russia – Traffic in Transit afirmou que a boa-fé limita o uso oportunista da exceção de segurança e permite controle objetivo de certos requisitos. [16] Essa orientação é relevante para a economia digital. Se todo serviço digital crítico puder ser restringido sob alegação genérica de segurança nacional, o sistema multilateral perde previsibilidade. Por outro lado, se a segurança digital for tratada como mero protecionismo, Estados ficarão sem instrumentos para proteger funções essenciais. O equilíbrio exige proporcionalidade, transparência, necessidade, boa-fé e distinção entre risco real e vantagem industrial disfarçada.

Há ainda o tema do comércio eletrônico. A discussão internacional sobre transmissões eletrônicas, tarifas digitais e regras plurilaterais demonstra que a economia digital ainda carece de regime multilateral robusto. [17] Países em desenvolvimento têm razão em apontar que a liberalização digital sem política de desenvolvimento pode perpetuar assimetrias de captura de valor. Países exportadores de serviços digitais têm razão em defender previsibilidade. A solução não está em fragmentar a internet, mas em construir regras que combinem abertura, tributação justa, concorrência, proteção de dados, desenvolvimento produtivo e salvaguardas para infraestrutura crítica.

6. Três modelos em disputa: hegemonia de mercado, soberania estatal centralizada e autonomia regulatória democrática

A geoeconomia digital contemporânea é frequentemente descrita como disputa entre Estados Unidos, China e União Europeia. A simplificação é útil, desde que não obscureça diferenças internas. O modelo norte-americano combina ecossistema privado altamente inovador, capital de risco, universidades, compras públicas de defesa, mercado financeiro profundo, proteção robusta de propriedade intelectual e capacidade estatal de impor sanções, controles de exportação e jurisdição extraterritorial. Sua narrativa pública

privilegia mercado e inovação, mas sua prática revela densa articulação entre Estado, segurança nacional e empresas líderes.

O modelo chinês articula soberania digital como controle nacional abrangente sobre infraestrutura, dados, plataformas, cadeias de suprimento e discurso público. A legislação chinesa de cibersegurança e proteção de informações pessoais utiliza linguagem de soberania do ciberespaço, segurança nacional e governança de dados, dentro de uma arquitetura política centralizada. [18] O resultado é capacidade industrial e operacional significativa, mas acompanhada de riscos profundos para liberdade de expressão, pluralismo, privacidade diante do Estado e controle social. Para democracias constitucionais, não se trata de copiar a China, mas de compreender que capacidade tecnológica sem garantias pode produzir soberania autoritária.

A União Europeia tenta construir uma terceira gramática: regulação baseada em direitos, mercado interno, concorrência, proteção de dados, segurança, valores democráticos e autonomia estratégica. O GDPR projetou globalmente um padrão de proteção de dados; o Digital Markets Act busca limitar o poder de gatekeepers; o Data Act procura disciplinar acesso e uso de dados; o AI Act cria uma arquitetura horizontal de riscos para sistemas de IA. [19][20][21] O pacote de soberania tecnológica e a proposta do Cloud and AI Development Act sinalizam uma transição: a União percebe que regulação sem capacidade industrial e computacional própria pode transformar-se em normatividade sem infraestrutura.

A experiência europeia é instrutiva porque revela a insuficiência tanto do laissez-faire quanto do constitucionalismo digital puramente regulatório. A proteção de dados, a transparência algorítmica e a concorrência são necessárias, mas não bastam se os modelos, chips e nuvens permanecem concentrados fora da jurisdição efetiva. Por isso, iniciativas de nuvem soberana, centros públicos de computação de IA, apoio a software livre, compras públicas estratégicas e políticas de semicondutores tornam-se complementos institucionais da regulação. [22][23][24]

O risco europeu, contudo, é converter soberania em rótulo comercial. A expressão “soberignity washing” descreve ofertas que prometem soberania apenas por data centers locais ou interfaces contratuais, sem controle efetivo de propriedade, jurisdição, chaves, cadeia de suprimentos, administração operacional e reversibilidade. Para evitar esse risco, a soberania deve ser testável. Uma nuvem ou IA só pode ser considerada soberana para funções críticas se passar por critérios verificáveis: controle de acesso; independência operacional; proteção contra ordens incompatíveis; portabilidade; auditoria; transparência de subcontratação; localização de chaves; plano de continuidade; e submissão integral a autoridades locais competentes.

Essa comparação demonstra que a soberania digital democrática precisa combinar a capacidade norte-americana de inovar, a consciência chinesa sobre infraestrutura e a gramática europeia de direitos, sem reproduzir os déficits de cada modelo: concentração privada sem accountability; centralização estatal sem liberdade; e regulação sofisticada sem base produtiva suficiente. Para países do Sul Global, a tarefa é ainda mais difícil, pois a restrição fiscal e tecnológica exige seletividade. Não se pode fazer tudo; é preciso escolher o mínimo soberano.

7. Brasil e Sul Global: do usuário de plataformas ao construtor de infraestrutura pública digital

O Brasil ocupa posição ambivalente. É grande mercado digital, possui sistema financeiro sofisticado, tradição regulatória relevante, base científica expressiva, matriz elétrica comparativamente limpa e exemplos bem-sucedidos de infraestrutura pública digital, como Pix e gov.br. Ao mesmo tempo, depende fortemente de nuvens estrangeiras, semicondutores importados, plataformas globais de comunicação, sistemas proprietários em órgãos públicos e modelos de IA desenvolvidos fora do país. A questão brasileira não é escolher entre integração global e soberania; é evitar que a integração se converta em dependência irreversível.

O Pix é o caso paradigmático. Ao criar uma camada pública de pagamento instantâneo, interoperável e regulada, o Banco Central reduziu custos de transação, abriu espaço para novos serviços, ampliou inclusão e diminuiu dependência de arranjos privados internacionais. [25] A própria referência ao Pix em investigação comercial norte-americana sob a Seção 301 revela que infraestrutura pública digital bem-sucedida pode ser percebida por atores externos como barreira competitiva. [26] Isso não significa que todo conflito regulatório seja agressão; significa que escolhas públicas de infraestrutura têm efeitos distributivos internacionais.

O aprendizado do Pix não deve ser romantizado. Sistemas de pagamento instantâneo também geram riscos: fraudes, engenharia social, assimetria informacional, concentração de dados financeiros e pressão por integração com novos serviços. Estudos recentes sobre fraude no Pix destacam que a sofisticação dos ataques exige defesas adaptativas e educação permanente do usuário. [27] A lição correta, portanto, é dupla: infraestrutura pública digital pode criar valor soberano, mas precisa de segurança, governança, capacidade técnica e revisão contínua.

A agenda brasileira deveria partir de uma classificação de criticidade. Nem todo sistema público demanda nuvem integralmente soberana. Uma página informativa de baixo risco não possui a mesma relevância que prontuários de saúde, bases biométricas, cadastros sociais, dados fiscais, sistemas judiciais, comunicações sensíveis, segurança pública, operações do Banco Central e modelos de IA incorporados a decisões administrativas. A política deve distinguir níveis de sensibilidade, aplicando requisitos mais rígidos onde a falha, a exposição ou o desligamento produzirem dano institucional grave.

Para o Sul Global, soberania digital também é questão de desenvolvimento. A dependência de plataformas estrangeiras pode produzir comodidade no curto prazo e subdesenvolvimento produtivo no longo prazo. Quando o Estado compra soluções fechadas, sem transferência de conhecimento, sem exigência de interoperabilidade e sem possibilidade de auditoria, ele financia a aprendizagem alheia e enfraquece a sua própria. A política pública deve criar demanda para empresas locais e regionais, universidades, consórcios, software livre, padrões abertos e laboratórios públicos. Essa orientação não é protecionismo vulgar; é política de aprendizagem. [28][29][30]

A questão energética dos data centers merece atenção especial. A expansão de instalações intensivas em energia pode ser oportunidade para investimento, empregos e inserção em cadeias globais. Porém, se o país apenas oferece energia limpa barata, isenções e território, sem governança sobre uso, contrapartidas tecnológicas, eficiência hídrica, critérios ambientais, integração produtiva local e tributação adequada, poderá subsidiar emissões evitadas de empresas estrangeiras sem capturar valor proporcional.

Soberania digital ambientalmente responsável exige que infraestrutura de dados seja tratada como infraestrutura crítica, não como empreendimento imobiliário ordinário.

8. Compras públicas como política de soberania: demanda, padrões e aprendizagem

As compras governamentais constituem um dos instrumentos mais poderosos e subutilizados da soberania digital. Estados compram nuvem, softwares, sistemas de gestão, segurança, equipamentos, consultorias, IA, armazenamento e serviços de dados. Cada contrato público decide, ainda que silenciosamente, se o país aprofunda lock-in proprietário ou constrói capacidade. A pergunta central da contratação pública digital não deve ser apenas qual proposta é mais barata no dia da licitação, mas qual arquitetura reduz custo total de dependência ao longo do ciclo de vida.

A teoria econômica da inovação demonstra que o Estado pode criar mercados, coordenar expectativas, financiar risco e orientar trajetórias tecnológicas. [31] A compra pública, nesse sentido, não é gasto passivo; é sinal de demanda. Quando editais exigem padrões abertos, interoperabilidade, documentação, transferência de conhecimento, escrow de código em casos críticos, portabilidade de dados, APIs públicas, auditoria algorítmica, localização de chaves e cláusulas de saída, o Estado molda o mercado. Quando aceita soluções fechadas, renova contratos por inércia e terceiriza sua inteligência institucional, também molda o mercado — mas na direção da dependência.

A soberania por compras públicas deve obedecer a critérios de proporcionalidade. Exigir fornecedor nacional para qualquer serviço de baixa criticidade pode aumentar custos e reduzir qualidade sem ganho soberano. Por outro lado, permitir dependência estrangeira irreversível em sistemas críticos pode ser economicamente eficiente apenas na aparência. O cálculo correto deve incorporar risco geopolítico, custo de migração, poder de barganha futuro, perda de conhecimento interno, exposição a sanções, vulnerabilidade de dados, efeitos concorrenciais e possibilidade de inovação local. Em infraestrutura crítica, o preço nominal raramente representa o custo real.

O contrato público digital soberano deveria incluir, ao menos, dez cláusulas estruturais: reversibilidade e portabilidade integral; interoperabilidade por padrões abertos; transparência de subcontratados; controle local de chaves e identidades; trilhas de auditoria; obrigação de continuidade e plano de contingência; matriz de riscos geopolíticos e regulatórios; vedação de uso secundário de dados públicos sem autorização; treinamento de equipes públicas; e penalidades por lock-in abusivo. Em sistemas de IA, devem somar-se explicabilidade adequada ao contexto, avaliação de impacto, registro de datasets relevantes, gestão de vieses, supervisão humana e mecanismos de contestação.

Essa agenda dialoga com a infraestrutura pública digital. O G20 descreveu a DPI como conjunto de sistemas compartilhados, mínimos e reutilizáveis, desenhados para interoperabilidade e adaptação a contextos nacionais. [32] A virtude dessa abordagem é evitar que cada órgão compre soluções isoladas. Identidade, pagamentos, assinatura, consentimento, autenticação, mensageria segura, interoperabilidade de dados e nuvem crítica podem ser tratados como camadas comuns. O Estado deixa de comprar ilhas e passa a construir estradas digitais.

9. Inteligência artificial soberana: capacidade, risco e democracia

A inteligência artificial exige tratamento específico porque combina três características: é tecnologia de propósito geral; depende de infraestrutura concentrada; e opera sobre linguagem, classificação e decisão. Um país pode usar IA estrangeira para tarefas ordinárias sem dano relevante. O problema surge quando modelos externos passam a mediar políticas públicas, decisões administrativas, segurança, justiça, saúde, educação ou comunicação governamental sem governança adequada. A soberania de IA não implica desenvolver nacionalmente todos os modelos de fronteira; implica saber quando, como e sob quais garantias modelos podem ser usados em funções críticas.

O AI Act europeu representa tentativa pioneira de regular sistemas de IA por risco, criando obrigações para sistemas de alto risco e regras específicas para modelos de propósito geral. [33][34] Sua importância não está apenas no conteúdo, mas na mudança de paradigma: a IA deixa de ser vista como produto neutro e passa a ser tratada como sistema sociotécnico com efeitos jurídicos. Para países como o Brasil, a experiência europeia sugere que a regulação deve combinar princípios, classificação de risco, obrigações de documentação, supervisão, transparência, governança de dados e sanções proporcionais.

Entretanto, a regulação de IA sem capacidade computacional tende a depender dos próprios regulados. Se autoridades públicas não têm acesso a infraestrutura, pessoal técnico, datasets de teste, ambientes seguros e modelos alternativos, a fiscalização será documental e reativa. A soberania de IA exige capacidade pública mínima: laboratórios de avaliação, centros de computação, parcerias universitárias, repositórios de benchmarks em língua portuguesa e contextos nacionais, formação de servidores, protocolos de aquisição e mecanismos independentes de auditoria. [35]

A democracia é condição, não obstáculo, da soberania digital. O risco de uma agenda soberanista é justificar vigilância, censura ou concentração estatal de dados em nome da autonomia nacional. A alternativa democrática exige que infraestruturas soberanas sejam acompanhadas por legalidade estrita, finalidade determinada, minimização de dados, transparência, órgãos independentes, controle judicial, participação social, segurança da informação e direito de contestação. A soberania digital que protege o Estado contra plataformas estrangeiras, mas entrega o cidadão a uma máquina estatal opaca, é juridicamente insuficiente e politicamente perigosa.

O constitucionalismo digital contemporâneo deve, portanto, equilibrar três polos: autonomia coletiva, liberdade individual e abertura econômica. Julie Cohen demonstra que o capitalismo informacional é construído juridicamente por regimes de propriedade, contrato, vigilância e plataformas. [36] Zuboff descreve a extração comportamental como nova lógica de acumulação. [37] Hildebrandt alerta para a transformação do direito diante de tecnologias inteligentes. [38] A conclusão comum é que a infraestrutura digital não pode ser deixada à autorregulação privada nem ao decisionismo estatal. Ela requer instituições.

10. Matriz normativa de soberania digital democrática

A partir da análise desenvolvida, é possível propor uma matriz normativa de soberania digital democrática. O primeiro critério é a criticidade. Quanto maior o impacto de interrupção, manipulação, exposição ou captura de determinado sistema sobre direitos fundamentais e funções públicas, maior deve ser o grau de controle público, redundância e exigência regulatória. Criticidade não é sinônimo de sigilo. Um sistema pode ser público e crítico, como pagamentos ou identidade; pode ser sigiloso e não sistêmico; pode ser ordinário e substituível. A classificação deve ser técnica, jurídica e revisável.

O segundo critério é a reversibilidade. Dependência digital se torna soberanamente perigosa quando não há saída real. Contratos sem portabilidade, dados em formatos proprietários, integrações opacas, customizações não documentadas, ausência de equipe interna e multas de rescisão desproporcionais criam servidão tecnológica. A reversibilidade deve ser princípio de contratação pública digital: nenhum fornecedor de infraestrutura crítica deve possuir poder de tornar sua substituição materialmente inviável.

O terceiro critério é a interoperabilidade. Padrões abertos não são detalhe técnico, mas garantia institucional contra monopólio. Interoperabilidade permite competição, continuidade, fiscalização e inovação incremental. O Digital Markets Act europeu expressa, em outro plano, a preocupação com gatekeepers capazes de controlar acesso a mercados digitais. [39] Em infraestrutura pública, o raciocínio é ainda mais forte: sistemas financiados com recursos públicos devem maximizar reutilização, integração e auditabilidade.

O quarto critério é a jurisdição efetiva. A autoridade nacional deve poder aplicar sua lei, proteger dados, investigar incidentes, impor sanções e assegurar continuidade. Isso não exige excluir fornecedores estrangeiros, mas exige desenho contratual e técnico compatível com o direito local. Para sistemas sensíveis, jurisdição efetiva pode demandar chaves sob controle local, operação por entidade submetida apenas à lei nacional ou acordos internacionais específicos. Para sistemas ordinários, podem bastar garantias contratuais e certificações.

O quinto critério é a auditabilidade. Sistemas públicos digitais precisam deixar rastros verificáveis de decisão, acesso, alteração, treinamento, inferência e compartilhamento. A auditabilidade não implica abertura indiscriminada de segredos de segurança ou propriedade intelectual; implica mecanismos proporcionais que permitam a autoridades competentes e, quando cabível, à sociedade, verificar conformidade, discriminação, segurança e finalidade. Sem auditoria, soberania vira confiança cega.

O sexto critério é a captura de valor público. Dados e infraestruturas públicas não devem subsidiar exclusivamente modelos privados de extração. Sempre que recursos públicos financiarem bases, APIs, modelos, infraestrutura ou integração, deve haver retorno social: padrões abertos, capacitação, transferência de conhecimento, estímulo a ecossistemas locais, publicização de componentes não sensíveis e proteção contra apropriação exclusiva. A soberania digital democrática não é apenas defensiva; é produtiva.

O sétimo critério é a compatibilidade com direitos fundamentais. Soberania digital sem proteção de direitos degenera em soberania de vigilância. O Global Digital Compact e os instrumentos internacionais de direitos humanos reafirmam que o espaço digital deve respeitar direitos, inclusão e governança responsável. [40][41] A infraestrutura soberana deve ser desenhada com privacidade, não discriminação, acessibilidade, segurança, devido processo e controle democrático desde sua origem.

11. Direito internacional econômico e cooperação: soberania sem fragmentação

Uma objeção recorrente sustenta que a soberania digital fragmentaria a internet e reduziria eficiência. A objeção procede quando soberania é confundida com fechamento, censura ou incompatibilidade técnica deliberada. Não procede quando soberania é definida como capacidade de governar dependências críticas dentro de uma economia aberta. A soberania democrática aqui defendida é aberta: privilegia padrões interoperáveis,

cooperação internacional, portabilidade, concorrência e acordos de reconhecimento. Ela combate a fragmentação produzida por monopólios e sanções arbitrárias, não a integração baseada em regras.

O direito internacional deve evoluir para reconhecer infraestruturas digitais críticas como objeto de cooperação específica. Assim como há regimes para aviação civil, telecomunicações, finanças, saúde e energia, deve haver regras mais densas sobre continuidade de serviços digitais essenciais, proteção de instituições internacionais contra sanções tecnológicas, acesso equitativo a capacidades computacionais, governança de IA, segurança cibernética, fluxos de dados para desenvolvimento e responsabilidade de plataformas sistêmicas. A pluralidade normativa será inevitável; a tarefa é ordená-la. [42][43]

A cooperação Sul-Sul tem papel estratégico. Países que compartilham vulnerabilidades semelhantes podem desenvolver padrões abertos, repositórios de software público, modelos de linguagem adaptados a línguas e contextos locais, nuvens federadas regionais, centros de avaliação de IA, mecanismos de compras conjuntas e cláusulas contratuais padronizadas. A soberania digital de países médios e em desenvolvimento será mais viável por consórcios do que por autossuficiência isolada.

Essa cooperação deve incorporar desenvolvimento como liberdade, não apenas como crescimento tecnológico. [44] A pergunta sobre soberania digital é, ao final, pergunta sobre capacidades: capacidade de o cidadão acessar serviços; de contestar decisões automatizadas; de participar da vida pública; de o Estado proteger direitos; de empresas locais inovarem; de universidades pesquisarem; de comunidades preservarem seus dados e culturas; e de sociedades escolherem seu futuro tecnológico. A infraestrutura digital deve expandir liberdades, não apenas acelerar transações.

12. Conclusão

A soberania digital é uma das categorias centrais do direito público e da economia política do século XXI. Ela nasce da constatação de que o poder contemporâneo se organiza por infraestruturas. Estados formalmente soberanos podem tornar-se funcionalmente dependentes quando suas políticas públicas, seus dados, seus pagamentos, sua comunicação, sua segurança e suas capacidades cognitivas dependem de plataformas, nuvens, chips e modelos sujeitos a decisões externas. A questão não é rejeitar a interdependência, mas governá-la.

Este artigo sustentou que soberania digital não é autarquia tecnológica. É capacidade institucional de controlar o mínimo crítico, preservar reversibilidade, assegurar continuidade, proteger direitos, estimular competição e capturar valor público. Trata-se de soberania proporcional: mais exigente em sistemas críticos, mais flexível em usos ordinários. Trata-se de soberania aberta: baseada em padrões, interoperabilidade e cooperação, não em isolamento. E trata-se de soberania democrática: limitada por direitos fundamentais, transparência, controle e finalidade pública.

A experiência recente de controles de exportação de IA, sanções extraterritoriais, Cloud Act, iniciativas europeias de autonomia tecnológica, debates na OMC e o caso brasileiro do Pix mostram que a infraestrutura digital se tornou campo de disputa geoeconômica. O Estado que não compreende essa transformação comprará dependência como se comprasse eficiência. O Estado que a compreende poderá usar regulação, compras

públicas, política industrial, cooperação internacional e infraestrutura pública digital para reconstruir capacidade sem fechar a economia e sem sacrificar liberdades.

O futuro da soberania não será decidido apenas em constituições, tratados ou tribunais. Será decidido também em editais de nuvem, padrões de API, data centers, chaves criptográficas, modelos de IA, sistemas de pagamento, políticas de semicondutores, contratos de software e arquiteturas de dados. A tarefa jurídica consiste em tornar visível essa infraestrutura, submetê-la ao direito e orientá-la ao desenvolvimento democrático. O desafio econômico consiste em transformar dependência em aprendizagem, compra pública em mercado, dado em valor social e inovação em capacidade coletiva. Soberania digital, nesse sentido, é a arte institucional de manter aberta a possibilidade de decidir.

Referências bibliográficas

ACEMOGLU, Daron; ROBINSON, James A. Why Nations Fail: The Origins of Power, Prosperity, and Poverty. New York: Crown, 2012.

ANTHROPIC. Statement on the US government directive to suspend access to Fable 5 and Mythos 5. 12 jun. 2026. Disponível em: https://www.anthropic.com/news/fable-mythos-access. Acesso em: 24 jun. 2026.

ASSOCIATED PRESS. Trump's sanctions on ICC prosecutor have halted tribunal's work, officials and lawyers say. 15 maio 2025.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 1, de 12 de agosto de 2020. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento. Brasília: BCB, 2020.

BANCO CENTRAL DO BRASIL. Estatísticas do Pix. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix-em-numeros-estatisticas. Acesso em: 24 jun. 2026.

BRATTON, Benjamin H. The Stack: On Software and Sovereignty. Cambridge, MA: MIT Press, 2015.

BRESNAHAN, Timothy F.; TRAJTENBERG, Manuel. General Purpose Technologies: 'Engines of Growth'? Journal of Econometrics, v. 65, n. 1, p. 83-108, 1995.

BURI, Ilaria; VAN HOBOKEN, Joris. The Digital Services Act (DSA) Proposal: A Critical Overview. Amsterdam Law School Research Paper, 2021.

CAMPOS MELLO, Patrícia. EUA podem apertar 'botão de desligar' IA no mundo, e soberania digital é urgente, diz Francesca Bria. Folha de S.Paulo, São Paulo, 23 jun. 2026.

CHINA. Cybersecurity Law of the People's Republic of China. Adopted 7 nov. 2016, effective 1 jun. 2017.

CHINA. Personal Information Protection Law of the People's Republic of China. Adopted 20 ago. 2021, effective 1 nov. 2021.

COHEN, Julie E. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford University Press, 2019.

DELMAS-MARTY, Mireille. Ordering Pluralism: A Conceptual Framework for Understanding the Transnational Legal World. Oxford: Hart Publishing, 2009.

DRAHOS, Peter. A Philosophy of Intellectual Property. Aldershot: Dartmouth, 1996.

DRAHOS, Peter; BRAITHWAITE, John. Information Feudalism: Who Owns the Knowledge Economy? London: Earthscan, 2002.

EUROPEAN COMMISSION. Proposal for the Cloud and AI Development Act (CADA). Brussels, 3 jun. 2026. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada. Acesso em: 24 jun. 2026.

EUROPEAN COMMISSION. EU Digital Decade Policy Programme 2030. Decision (EU) 2022/2481 of the European Parliament and of the Council, 14 dez. 2022.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, 4 maio 2016.

EUROPEAN UNION. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act). Official Journal of the European Union, 21 set. 2022.

EUROPEAN UNION. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union, 27 out. 2022.

EUROPEAN UNION. Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, 22 dez. 2023.

EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 jul. 2024.

FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, v. 44, n. 1, p. 42-79, 2019.

FLORIDI, Luciano. The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford: Oxford University Press, 2014.

FREEMAN, Christopher; SOETE, Luc. The Economics of Industrial Innovation. 3. ed. London: Routledge, 1997.

G20. G20 Framework for Systems of Digital Public Infrastructure. Digital Economy Ministers Meeting, Annex I, 19 ago. 2023.

G20. Maceió Ministerial Declaration on Digital Inclusion for All. 13 set. 2024.

HILDEBRANDT, Mireille. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar, 2015.

KEOHANE, Robert O.; NYE, Joseph S. Power and Interdependence. 4. ed. Boston: Longman, 2012.

KOSKENNIEMI, Martti. The Politics of International Law. Oxford: Hart Publishing, 2011.

KRASNER, Stephen D. Sovereignty: Organized Hypocrisy. Princeton: Princeton University Press, 1999.

LESSIG, Lawrence. Code: Version 2.0. New York: Basic Books, 2006.

LIU, Jingwen; LEE, Jyh-An. Strategic Stalemates: The Paradox of Export Controls in the U.S.-China AI Race. arXiv:2605.23475, 2026.

MAZZUCATO, Mariana. The Entrepreneurial State: Debunking Public vs. Private Sector Myths. London: Anthem Press, 2013.

MAZZUCATO, Mariana. Mission Economy: A Moonshot Guide to Changing Capitalism. New York: Harper Business, 2021.

MISHRA, Neha. Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? World Trade Review, v. 19, n. 3, p. 341-364, 2020.

NAGAR, Sarosh; EAVES, David. Interactions Between Artificial Intelligence and Digital Public Infrastructure: Concepts, Benefits, and Challenges. arXiv:2412.05761, 2024.

NORTH, Douglass C. Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press, 1990.

OECD. Digital Public Infrastructure for Digital Governments. OECD Public Governance Policy Papers, n. 68. Paris: OECD Publishing, 2024.

OECD. The Path to Becoming a Data-Driven Public Sector. OECD Digital Government Studies. Paris: OECD Publishing, 2019.

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE. Section 301 Investigation of Brazil's Acts, Policies, and Practices Related to Digital Trade and Electronic Payment Services. Washington, DC, 2025-2026.

PIZZOLATO, Glener Lanes; LOPES, Brenda Medeiros; SCHEPKE, Claudio; KREUTZ, Diego. A Taxonomy of Pix Fraud in Brazil: Attack Methodologies, AI-Driven Amplification, and Defensive Strategies. arXiv:2511.20902, 2025.

RODRIK, Dani. Industrial Policy for the Twenty-First Century. Cambridge, MA: Harvard Kennedy School, 2004.

RODRIK, Dani. The Globalization Paradox: Democracy and the Future of the World Economy. New York: W. W. Norton, 2011.

RODRIK, Dani. Straight Talk on Trade: Ideas for a Sane World Economy. Princeton: Princeton University Press, 2017.

SASSEN, Saskia. Territory, Authority, Rights: From Medieval to Global Assemblages. Princeton: Princeton University Press, 2006.

SEN, Amartya. Development as Freedom. New York: Alfred A. Knopf, 1999.

SMUHA, Nathalie A. The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence. Computer Law Review International, v. 20, n. 4, p. 97-106, 2019.

SOUSA E SILVA, Nuno. The Artificial Intelligence Act: Critical Overview. arXiv:2409.00264, 2024.

SRIVASTAVA, Swati; BULLOCK, Justin. AI, Global Governance, and Digital Sovereignty. arXiv:2410.17481, 2024.

STIGLITZ, Joseph E. The Price of Inequality. New York: W. W. Norton, 2012.

STIGLITZ, Joseph E.; GREENWALD, Bruce C. Creating a Learning Society. New York: Columbia University Press, 2014.

STRANGE, Susan. States and Markets. 2. ed. London: Pinter, 1994.

STRANGE, Susan. The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge: Cambridge University Press, 1996.

UNCTAD. Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. Geneva: United Nations, 2021.

UNCTAD. Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future. Geneva: United Nations, 2024.

UNITED NATIONS. Global Digital Compact. New York: United Nations, 2024.

UNITED NATIONS HUMAN RIGHTS COUNCIL. The promotion, protection and enjoyment of human rights on the Internet. A/HRC/32/L.20, 2016.

UNITED STATES. Clarifying Lawful Overseas Use of Data Act, Division V of the Consolidated Appropriations Act, 2018, Public Law 115-141, 23 mar. 2018.

UNITED STATES. Executive Order 14203: Imposing Sanctions on the International Criminal Court. Washington, DC, 6 fev. 2025.

WORLD BANK. Digital Public Infrastructure and Development: A World Bank Group Approach. Washington, DC: World Bank, 2025.

WTO. General Agreement on Trade in Services. Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1994.

WTO. Panel Report, Russia – Measures Concerning Traffic in Transit, WT/DS512/R, 5 abr. 2019.

WTO. Agreement on Electronic Commerce. Joint Statement Initiative on E-Commerce, 2024-2026.

WU, Tim. The Master Switch: The Rise and Fall of Information Empires. New York: Knopf, 2010.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

[1] CAMPOS MELLO, Patrícia. EUA podem apertar 'botão de desligar' IA no mundo, e soberania digital é urgente, diz Francesca Bria. Folha de S.Paulo, São Paulo, 23 jun. 2026; ANTHROPIC. Statement on the US government directive to suspend access to Fable 5 and Mythos 5. 12 jun. 2026. Disponível em: https://www.anthropic.com/news/fable-mythos-access. Acesso em: 24 jun. 2026.

[2] KRASNER, Stephen D. Sovereignty: Organized Hypocrisy. Princeton: Princeton University Press, 1999.

[3] KEOHANE, Robert O.; NYE, Joseph S. Power and Interdependence. 4. ed. Boston: Longman, 2012; FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, v. 44, n. 1, p. 42-79, 2019.

[4] BRATTON, Benjamin H. The Stack: On Software and Sovereignty. Cambridge, MA: MIT Press, 2015; LESSIG, Lawrence. Code: Version 2.0. New York: Basic Books, 2006.

[5] UNITED STATES. Clarifying Lawful Overseas Use of Data Act, Division V of the Consolidated Appropriations Act, 2018, Public Law 115-141, 23 mar. 2018; U.S. DEPARTMENT OF JUSTICE. The CLOUD Act. Washington, DC, 2019.

[6] KEOHANE, Robert O.; NYE, Joseph S. Power and Interdependence. 4. ed. Boston: Longman, 2012; FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, v. 44, n. 1, p. 42-79, 2019.

[7] STRANGE, Susan. States and Markets. 2. ed. London: Pinter, 1994; STRANGE, Susan. The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge: Cambridge University Press, 1996.

[8] UNCTAD. Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. Geneva: United Nations, 2021; UNCTAD. Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future. Geneva: United Nations, 2024.

[9] BRESNAHAN, Timothy F.; TRAJTENBERG, Manuel. General Purpose Technologies: ‘Engines of Growth’? Journal of Econometrics, v. 65, n. 1, p. 83-108, 1995.

[10] BANCO CENTRAL DO BRASIL. Resolução BCB nº 1, de 12 de agosto de 2020. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento; BANCO CENTRAL DO BRASIL. Estatísticas do Pix. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix-em-numeros-estatisticas. Acesso em: 24 jun. 2026.

[11] WORLD BANK. Digital Public Infrastructure and Development: A World Bank Group Approach. Washington, DC: World Bank, 2025; OECD. Digital Public Infrastructure for Digital Governments. OECD Public Governance Policy Papers, n. 68, Paris: OECD Publishing, 2024.

[12] KEOHANE, Robert O.; NYE, Joseph S. Power and Interdependence. 4. ed. Boston: Longman, 2012; FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, v. 44, n. 1, p. 42-79, 2019.

[13] UNITED STATES. Clarifying Lawful Overseas Use of Data Act, Division V of the Consolidated Appropriations Act, 2018, Public Law 115-141, 23 mar. 2018; U.S. DEPARTMENT OF JUSTICE. The CLOUD Act. Washington, DC, 2019.

[14] UNITED STATES. Executive Order 14203: Imposing Sanctions on the International Criminal Court. Washington, DC, 6 fev. 2025; ASSOCIATED PRESS. Trump's sanctions on ICC prosecutor have halted tribunal's work, officials and lawyers say. 15 maio 2025.

[15] LIU, Jingwen; LEE, Jyh-An. Strategic Stalemates: The Paradox of Export Controls in the U.S.-China AI Race. arXiv:2605.23475, 2026.

[16] WTO. General Agreement on Trade in Services, Article XIV bis; WTO. Panel Report, Russia – Measures Concerning Traffic in Transit, WT/DS512/R, 5 abr. 2019.

[17] WORLD TRADE ORGANIZATION. Agreement on Electronic Commerce. Joint Statement Initiative on E-Commerce, stabilized text and subsequent WTO materials, 2024-2026.

[18] CHINA. Cybersecurity Law of the People's Republic of China, adopted 7 nov. 2016, effective 1 jun. 2017; CHINA. Personal Information Protection Law of the People's Republic of China, adopted 20 ago. 2021, effective 1 nov. 2021.

[19] EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 jul. 2024.

[20] EUROPEAN UNION. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act). Official Journal of the European Union, 21 set. 2022; EUROPEAN UNION. Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, 22 dez. 2023.

[21] EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, 4 maio 2016.

[22] EUROPEAN COMMISSION. Proposal for the Cloud and AI Development Act (CADA). Brussels, 3 jun. 2026. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada. Acesso em: 24 jun. 2026.

[23] EUROPEAN COMMISSION. EU Digital Decade Policy Programme 2030. Decision (EU) 2022/2481 of the European Parliament and of the Council, 14 dez. 2022.

[24] EUROPEAN COMMISSION. EU Commission awards €180 million cloud contract to four European providers. Reuters, 17 abr. 2026; EUROPEAN COMMISSION. Cloud Sovereignty Framework, procurement materials, 2025-2026.

[25] BANCO CENTRAL DO BRASIL. Resolução BCB nº 1, de 12 de agosto de 2020. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento; BANCO CENTRAL DO BRASIL. Estatísticas do Pix. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix-em-numeros-estatisticas. Acesso em: 24 jun. 2026.

[26] OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE. Section 301 Investigation of Brazil's Acts, Policies, and Practices Related to Digital Trade and Electronic Payment Services. Washington, DC, 2025-2026.

[27] PIZZOLATO, Glener Lanes; LOPES, Brenda Medeiros; SCHEPKE, Claudio; KREUTZ, Diego. A Taxonomy of Pix Fraud in Brazil: Attack Methodologies, AI-Driven Amplification, and Defensive Strategies. arXiv:2511.20902, 2025.

[28] MAZZUCATO, Mariana. The Entrepreneurial State: Debunking Public vs. Private Sector Myths. London: Anthem Press, 2013; MAZZUCATO, Mariana. Mission Economy: A Moonshot Guide to Changing Capitalism. New York: Harper Business, 2021.

[29] FREEMAN, Christopher; SOETE, Luc. The Economics of Industrial Innovation. 3. ed. London: Routledge, 1997.

[30] RODRIK, Dani. Industrial Policy for the Twenty-First Century. Cambridge, MA: Harvard Kennedy School, 2004.

[31] MAZZUCATO, Mariana. The Entrepreneurial State: Debunking Public vs. Private Sector Myths. London: Anthem Press, 2013; MAZZUCATO, Mariana. Mission Economy: A Moonshot Guide to Changing Capitalism. New York: Harper Business, 2021.

[32] G20. G20 Framework for Systems of Digital Public Infrastructure. Digital Economy Ministers Meeting, Annex I, 19 ago. 2023; G20. Maceió Ministerial Declaration on Digital Inclusion for All. 13 set. 2024.

[33] EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 jul. 2024.

[34] SOUSA E SILVA, Nuno. The Artificial Intelligence Act: Critical Overview. arXiv:2409.00264, 2024.

[35] NAGAR, Sarosh; EAVES, David. Interactions Between Artificial Intelligence and Digital Public Infrastructure: Concepts, Benefits, and Challenges. arXiv:2412.05761, 2024.

[36] COHEN, Julie E. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford University Press, 2019.

[37] ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

[38] HILDEBRANDT, Mireille. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar, 2015.

[39] EUROPEAN UNION. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act). Official Journal of the European Union, 21 set. 2022; EUROPEAN UNION. Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, 22 dez. 2023.

[40] UNITED NATIONS. Global Digital Compact. New York: United Nations, 2024.

[41] BROWN, Ian; KORFF, Douwe. Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online. Global Network Initiative, 2012; UNITED NATIONS HUMAN RIGHTS COUNCIL. The promotion, protection and enjoyment of human rights on the Internet. A/HRC/32/L.20, 2016.

[42] DELMAS-MARTY, Mireille. Ordering Pluralism: A Conceptual Framework for Understanding the Transnational Legal World. Oxford: Hart Publishing, 2009.

[43] KOSKENNIEMI, Martti. The Politics of International Law. Oxford: Hart Publishing, 2011.

[44] SEN, Amartya. Development as Freedom. New York: Alfred A. Knopf, 1999.