

**Eduardo Carvalho
Nepomuceno Alencar**

GOVERNANÇA EM TEMPO REAL

como o Brasil pode parar de fingir que governa

2027

CAPÍTULO 8

CAPACIDADE ESTATAL DIGITAL: DA ENTREGA TECNOLÓGICA À CAPACIDADE PÚBLICA

Tecnologia pública costuma ser anunciada como projeto. Um novo sistema. Uma nova plataforma. Um novo aplicativo. Um novo portal. Um novo painel. Uma nova base integrada. Uma nova solução de inteligência artificial. O lançamento tem nome, identidade visual, cronograma, fornecedor, equipe e promessa.

O problema começa quando o projeto é confundido com capacidade.

Um sistema pode existir sem melhorar a decisão. Um painel pode ser atualizado sem orientar prioridade. Uma base pode ser integrada tecnicamente e continuar inútil para a gestão. Um portal pode modernizar a aparência do serviço e não resolver a exclusão de quem não consegue acessá-lo. Uma política de dados pode existir no papel e não alterar o comportamento das áreas. Uma infraestrutura digital pode ser implantada e, ainda assim, não produzir confiança, interoperabilidade, responsividade nem aprendizagem.

Capacidade estatal digital não é ter tecnologia. É ter instituições capazes de decidir, coordenar, implementar, medir, corrigir e prestar contas usando tecnologia.

Essa distinção é central. O Estado brasileiro não sofre apenas por falta de sistemas. Em muitas áreas, sofre por excesso de sistemas sem arquitetura comum, sem governança de dados, sem interoperabilidade, sem responsável claro, sem indicadores com consequência e sem rotina de aprendizagem. O problema não é apenas digitalizar pouco. É digitalizar de modo fragmentado, sem transformar informação em capacidade pública.

Este capítulo trata dessa passagem: quando tecnologia pública vira capacidade, e quando vira apenas projeto.

1. O FETICHE DO SISTEMA

Há uma cena recorrente na administração pública. Uma organização enfrenta um problema de coordenação, fila, controle, transparência ou desempenho. A resposta institucional aparece rapidamente: precisamos de um sistema.

Às vezes isso é verdade. Na maioria das vezes, não é suficiente.

O sistema se torna uma solução confortável porque materializa ação. Permite contratar, planejar, apresentar cronograma, demonstrar modernização, criar entregáveis visíveis e comunicar avanço. É mais fácil anunciar uma plataforma do que redesenhar responsabilidades. É mais fácil criar um painel do que definir quem decide diante do indicador. É mais fácil integrar bases do que resolver conflitos de competência entre órgãos. É mais fácil automatizar um formulário do que simplificar a regra que torna o serviço incompreensível.

O fetiche do sistema aparece quando a organização trata tecnologia como substituta de governança.

Isso produz uma forma específica de desperdício público. Não é o desperdício clássico de obra paralisada ou contrato inútil. É o desperdício de energia institucional em ferramentas que funcionam tecnicamente, mas não alteram a capacidade de resolver problemas. O sistema entra em produção, mas a fila continua. O painel fica atualizado, mas ninguém muda a agenda de gestão. A base é compartilhada, mas os órgãos continuam decidindo isoladamente. O aplicativo existe, mas o cidadão vulnerável continua dependendo de intermediários. A automação reduz etapas para alguns e cria barreiras para outros.

A Figura 8.1 resume a distinção entre entrega tecnológica e capacidade estatal digital, duas coisas que o discurso público frequentemente confunde.

Figura 8.1 – Entrega tecnológica versus capacidade estatal digital

ENTREGA TECNOLÓGICA	CAPACIDADE ESTATAL DIGITAL
Sistema implantado e em produção	Decisão melhorada pelo uso do sistema
Base de dados integrada	Análise transversal que orienta prioridade
Painel de indicadores publicado	Reunião de gestão que usa o painel para decidir
Serviço digitalizado	Serviço acessível a quem mais precisa
IA adotada	IA com governança, auditoria e consequência
Meta de cobertura digital cumprida	Desigualdade de acesso reduzida com evidência
Piloto de GovTech lançado	Piloto avaliado com critério e expandido com base em resultado

Fonte: Elaboração própria.

Tecnologia pública precisa ser julgada por valor público, não por entrega técnica isolada. O valor não está no sistema em si. Está na decisão melhor, no serviço mais acessível, no risco reduzido, no tempo economizado, na confiança aumentada, na desigualdade diminuída, na coordenação ampliada, na aprendizagem incorporada.

Sem essa mudança de critério, transformação digital vira modernização performática.

2. INFRAESTRUTURA PÚBLICA DIGITAL NÃO É PACOTE TECNOLÓGICO

A agenda internacional de *Digital Public Infrastructure* trouxe uma contribuição importante: ela desloca a discussão do aplicativo isolado para a infraestrutura compartilhada. Identidade digital, pagamentos, troca de dados, registros, interoperabilidade, autenticação, consentimento, segurança, padrões e APIs podem formar uma base comum para serviços públicos e inovação.

Mas há um risco: tratar DPI como se fosse apenas uma pilha técnica.

Infraestrutura pública digital deve ser entendida como infraestrutura de confiança. Ela precisa permitir que pessoas, governos, empresas e organizações interajam com segurança, previsibilidade, inclusão e *accountability*. Para isso, a dimensão técnica é indispensável, mas não basta. A Tabela 8.1 organiza as dimensões que uma DPI precisa contemplar para ser genuinamente pública.

Tabela 8.1 – Dimensões de uma infraestrutura pública digital genuína

Dimensão	O que exige	Risco se ausente
Técnica	Padrões abertos, APIs documentadas, escalabilidade, resiliência	Aprisionamento tecnológico; incapacidade de evolução
Governança	Regras de gestão, responsabilidades, comitês, revisão periódica	Fragmentação de decisões; ausência de <i>accountability</i>
Inclusão	Canais alternativos, acessibilidade, letramento, suporte presencial	Exclusão digital que amplifica desigualdade
Proteção de dados	LGPD, consentimento, minimização, finalidade, direitos dos titulares	Vigilância; uso indevido; erosão de confiança
Segurança cibernética	Gestão de vulnerabilidades, resposta a incidentes, continuidade	Ataques que paralisam serviços; vazamento de dados sensíveis

Dimensão	O que exige	Risco se ausente
Financiamento	Sustentabilidade fiscal, modelo de custeio, independência de fornecedor único	Descontinuidade; dependência de ciclos políticos
Avaliação	Métricas de uso, acesso, qualidade, impacto distributivo	Invisibilidade de falhas; ausência de aprendizagem
Governança de IA	Estrutura de supervisão, gestão de risco de modelos, explicabilidade proporcional ao risco, auditoria contínua, responsabilização por decisões automatizadas – seguindo padrões internacionais como os 12 <i>Sound Practices</i> do FSB (2026) e o AI Act da UE (2024)	Automação de decisões públicas sem <i>accountability</i> ; danos invisíveis por viés sistêmico; impossibilidade de contestação efetiva pelo cidadão

Fonte: Elaboração própria. Dimensão “Governança de IA” adicionada com base no FSB *Sound Practices for Responsible Adoption of AI* (jun. 2026) e no AI Act (Regulamento (UE) 2024/1689).

A agenda de *Digital Public Infrastructure* para cidades e comunidades reforça exatamente esse ponto. A mensagem mais importante não é que cidades precisam de mais tecnologia. É que precisam de infraestrutura digital inclusiva, escalável e interoperável, orientada a serviços públicos, confiança, sustentabilidade e implementação local.

O cidadão não vive em organogramas. Ele vive problemas integrados. Uma mãe que busca vaga em creche, atendimento de saúde, benefício social e transporte não deveria precisar compreender a fragmentação administrativa do Estado. Um empreendedor que tenta regularizar uma atividade não deveria atravessar labirintos digitais que reproduzem burocracias antigas. Um gestor municipal que precisa agir diante de enchentes, calor extremo ou insegurança alimentar não deveria depender de bases isoladas e desatualizadas.

DPI faz sentido quando reduz essa fragmentação. Mas, se implantada sem governança, pode reforçar os mesmos problemas que pretende resolver: dependência de fornecedores, exclusão digital, concentração de dados, vigilância sem controle, custos recorrentes e plataformas que não conversam.

Infraestrutura digital só é pública de verdade quando serve ao valor público sob regras públicas.

3. BENCHMARKS INTERNACIONAIS: O QUE O BRASIL PODE APRENDER

Três experiências internacionais são especialmente relevantes para o debate brasileiro sobre capacidade estatal digital.

A Estônia é o caso mais citado, e o mais mal interpretado. O país não digitalizou porque possuía tecnologia avançada. Digitalizou porque tomou decisões institucionais radicais: identidade digital única para todos os cidadãos, interoperabilidade obrigatória entre órgãos públicos, princípio de *once only* (o Estado coleta o dado uma vez e nunca o repete), arquitetura de segurança distribuída e governança pública sólida. O resultado, construído ao longo de décadas, é um Estado que usa dados de forma coordenada, segura e auditável. A lição não é copiar a tecnologia estoniana. É entender que capacidade digital foi tratada como prioridade de governança do Estado, não como projeto de TI. E que a arquitetura técnica foi deliberadamente desenhada para evitar pontos únicos de falha, uma decisão motivada por preocupações de segurança nacional que se revelou também uma excelente prática de resiliência operacional.

O *Government Digital Service* do Reino Unido introduziu uma cultura de produto no governo federal. Em vez de contratar grandes sistemas monolíticos, o GDS promoveu desenvolvimento incremental, interfaces centradas no usuário, padrões comuns, documentação aberta e avaliação contínua. A frase que guiou a agenda, “*make things open: it makes things better*”, expressa uma filosofia que vai além de código aberto: abertura como disciplina de qualidade, de aprendizagem e de *accountability*. O GDS também introduziu uma prática que o Brasil ainda aplica de forma desigual: times multidisciplinares permanentes com gestores de produto, designers de serviço, engenheiros e especialistas em política pública trabalhando juntos, não sequencialmente. A lição é que governança digital madura não é sobre ter o melhor sistema, mas sobre ter processos que produzem sistemas melhores com o tempo.

A Índia construiu o sistema UIDAI de identidade biométrica (Aadhaar) com escala impressionante, mais de um bilhão de registros, e aprendeu lições duras sobre os riscos de sistemas sem salvaguardas suficientes. O Aadhaar expandiu o acesso a serviços para populações antes excluídas do sistema bancário e de benefícios. Mas também gerou exclusões indevidas, falhas de autenticação em contextos de baixa conectividade e debates substantivos sobre privacidade, vigilância e concentração de poder. A lição indiana é duplamente importante: DPI pode escalar transformação inclusiva, e DPI sem proteção de direitos pode produzir novos sistemas de exclusão com aparência de modernização.

O Brasil tem seu próprio conjunto de experiências relevantes. O Pix, sistema de pagamentos instantâneos do Banco Central, tornou-se referência global de DPI financeira: *open source*, interoperável, acessível por qualquer instituição financeira regulada, com crescimento acelerado de adoção e impacto mensurável sobre inclusão financeira. O gov.br, portal unificado de serviços digitais federais, avançou na integração da identidade digital e na oferta de

serviços por canal único, embora a experiência do usuário ainda seja desigual entre serviços. A RNDS, Rede Nacional de Dados em Saúde, criou a infraestrutura de interoperabilidade para troca de dados entre estabelecimentos, estados e o nível federal, com desafios conhecidos de adesão e qualidade dos dados.

O Judiciário oferece um quarto caso brasileiro relevante, mais setorial. O sistema VICTOR, do Supremo Tribunal Federal, usa IA para triar e classificar recursos segundo o requisito de repercussão geral, e é citado em diretrizes da UNESCO de 2025 sobre uso de IA em cortes e tribunais como exemplo de aplicação concreta ao lado de um caso colombiano de decisão judicial assistida por IA. As diretrizes propõem quinze princípios organizados em dois níveis, o institucional, para organizações judiciais que adotam sistemas, e o individual, para magistrados e servidores que usam ferramentas no dia a dia, incluindo IA generativa. A distinção importa: um tribunal pode ter um sistema de triagem bem governado no nível institucional e, ao mesmo tempo, ter juízes usando IA generativa de forma não regulada nos gabinetes. Governança de IA no setor público não é uma política única. É uma política institucional e uma política de uso individual operando ao mesmo tempo, com exigências distintas.

Dois indicadores internacionais recentes ajudam a situar o Brasil nesse quadro, e a tensão entre eles é o ponto mais instrutivo. O Global Index on Responsible AI, em sua segunda edição de 2026, avalia 135 países e coloca o Brasil na 11ª posição global, com pontuação 63,3 em 100, o primeiro lugar entre os países da América do Sul e Central. O destaque é qualificado: o Brasil está entre os poucos países que combinam framework formal e implementação real de governança de IA, quando a maioria dos países do Sul Global tem um ou outro, raramente os dois, a InovaCPIN, plataforma de compras públicas de inovação mantida pela ABDI em conjunto com o TCU, é um exemplo concreto dessa implementação, e a Estratégia Brasileira de IA passou a exigir que compras públicas de IA considerem transparência e proteção de dados, não apenas eficiência técnica. Ao mesmo tempo, o IMD World Competitiveness Yearbook 2026 mostra o Brasil caindo para a 65ª posição entre 70 economias, pior resultado da série recente e queda de sete posições em relação a 2025, com piora simultânea nos quatro pilares medidos, desempenho econômico, eficiência do governo, eficiência empresarial e infraestrutura. As duas medições não se contradizem. Descrevem o mesmo país por ângulos diferentes: capaz de construir ilhas de governança setorial sofisticada, compras de IA, pagamentos instantâneos, triagem judicial, enquanto a capacidade estatal de base, a que sustenta esses avanços pontuais, se deteriora. Ilhas de excelência não substituem capacidade

estatal ampla. Em algum momento, a fragilidade da base compromete até as ilhas.

Essas experiências demonstram que o país tem capacidade de construir DPI de nível mundial quando há mandato político, financiamento adequado, equipe técnica dedicada e governança clara. O desafio é generalizar essa capacidade para além dos casos mais favoráveis.

O quadro comparativo mais amplo disponível hoje reforça esse ponto e acrescenta uma advertência. O World Development Report 2026 do Banco Mundial, dedicado à promessa da inteligência artificial, organiza o argumento em torno de três elementos: capacidades, concentração e complementos institucionais. Sua tese central para países em desenvolvimento é que o caminho de valor não passa por competir na fronteira dos modelos, e sim por adaptar tecnologia a necessidades locais e construir os complementos institucionais que convertem capacidade técnica em desenvolvimento. O relatório separa três papéis do Estado que costumam ser tratados como um só: governo como habilitador de infraestrutura, competências e ecossistema; governo como usuário, com capacidade de equipe, dados preparados para IA, monitoramento de desempenho e supervisão de compras; e governo como regulador, com leis, enforcement e cooperação internacional.

Duas recomendações do relatório contrariam intuições correntes no debate brasileiro. A primeira é que, na prestação de serviços públicos, usos preditivos e de retaguarda tendem a ser preferíveis a interfaces generativas na linha de frente, porque são mais confiáveis onde o erro tem custo direto sobre o cidadão. A segunda é que soberania tecnológica não deve ser confundida com construir toda a cadeia localmente: o relatório favorece adaptação e interoperabilidade. Para um país que já demonstrou capacidade de construir infraestrutura pública digital de nível mundial, a advertência é pertinente. A escolha entre depender de tudo e construir tudo é falsa, e tratá-la como verdadeira consome recursos que fariam mais diferença na camada de capacidade institucional.

O denominador comum de todas essas experiências, nacionais e internacionais, é que capacidade digital foi construída, não apenas adquirida. Isso exige tempo, decisão política, investimento público, capacidade técnica interna, padrões compartilhados, avaliação contínua e disposição de aprender com o que falhou.

4. INTEROPERABILIDADE É GOVERNANÇA, NÃO CABO

Interoperabilidade costuma ser tratada como problema técnico. Sistemas precisam conversar. Bases precisam trocar dados. APIs precisam funcionar. Padrões precisam ser definidos. Tudo isso é verdade.

Mas a parte mais difícil da interoperabilidade raramente está no cabo, no *endpoint* ou no formato do arquivo. Está na governança.

Interoperar significa que organizações distintas aceitam coordenar conceitos, responsabilidades, padrões, permissões, ritmos e consequências. Uma secretaria precisa confiar nos dados de outra. Um órgão precisa aceitar atualizar cadastros que outros usarão. Uma área jurídica precisa autorizar fluxos seguros. Uma área de tecnologia precisa documentar e manter padrões. Gestores precisam abrir mão de soluções isoladas em favor de arquitetura comum. Fornecedores precisam operar dentro de regras que evitem aprisionamento.

Por isso interoperabilidade é uma decisão institucional antes de ser integração técnica.

O Brasil acumulou experiências valiosas nessa área. A REDESIM, Rede Nacional para a Simplificação do Registro e da Legalização de Empresas e Negócios, exemplifica o quanto interoperabilidade é difícil quando envolve múltiplos entes federativos com competências distintas: federal, estadual e municipal, cada um com sistemas próprios e ritmos diferentes de modernização. O Cadastro Base do Cidadão e a Rede Nacional de Dados em Saúde mostram que é possível avançar em interoperabilidade setorial com mandato claro, financiamento e arquitetura adequada, e também que os principais gargalos são quase sempre de governança, não de tecnologia.

A lição mais consistente dessas experiências é que interoperabilidade exige um responsável com autoridade real para resolver conflitos entre órgãos. Quando nenhuma instância tem poder de exigir aderência a padrões comuns, cada órgão adota seu próprio formato, seu próprio calendário de atualização e seus próprios critérios de qualidade. O resultado é um ecossistema tecnicamente conectável, mas praticamente fragmentado.

A Lei Geral de Proteção de Dados, LGPD, adicionou uma camada essencial a essa discussão. Dados pessoais têm titulares com direitos. Finalidade, minimização, consentimento, segurança, transparência e responsabilização são princípios que devem guiar qualquer integração de bases que envolva dados de cidadãos. A LGPD não é obstáculo à interoperabilidade. É sua condição de legitimidade.

Na prática, a articulação entre interoperabilidade e proteção de dados ainda é um gargalo. Muitas iniciativas de compartilhamento de dados no setor público avançam na dimensão técnica e ficam para trás na dimensão jurídica, sem análise de impacto à proteção de dados, sem definição de finalidade específica, sem mecanismos de contestação para o cidadão e sem trilha de auditoria que permita verificar como o dado foi usado.

Uma governança séria de interoperabilidade precisa responder a perguntas objetivas: quais dados são essenciais? Quem é autoridade sobre cada dado? Qual é a qualidade mínima aceitável? Quem pode acessar? Para qual finalidade? Como registrar uso? Como corrigir erro? Como proteger privacidade? Como garantir continuidade? Como medir o valor público gerado pela integração?

Capacidade digital madura sabe trabalhar com essa ambivalência. Não usa risco como justificativa para paralisar. Também não usa inovação como justificativa para ignorar salvaguardas.

5. CIBERSEGURANÇA COMO QUESTÃO DE GOVERNANÇA

A transformação digital do Estado amplia a superfície de ataque. Quanto mais serviços migram para o digital, quanto mais bases se integram, quanto mais dados sensíveis circulam em sistemas, maior é o risco de incidentes cibernéticos. Esse risco não é hipotético.

Ataques a sistemas de saúde, ministérios, tribunais, câmaras municipais e prefeituras têm se tornado frequentes no Brasil e no mundo. Dados de cidadãos vazam. Sistemas de atendimento ficam fora do ar. Informações sigilosas são comprometidas. Operações são paralisadas. Em casos documentados, dados de beneficiários de programas sociais, contribuintes, pacientes e litigantes foram expostos.

A cibersegurança no setor público ainda é tratada, em muitos órgãos, como problema de TI. Não é. É questão de governança.

Decisões de cibersegurança afetam quem pode acessar sistemas críticos, como credenciais são gerenciadas, quando *patches* de segurança são aplicados, como incidentes são detectados e respondidos, o que acontece com dados em caso de violação, quem notifica titulares e qual é a cadeia de responsabilidade quando algo falha. Essas são decisões com impacto direto sobre direitos, serviços e finanças públicas.

Um *framework* mínimo de cibersegurança para o setor público precisa cobrir: gestão de identidades e acessos com princípio de menor privilégio; monitoramento contínuo de sistemas críticos; plano de resposta a incidentes testado e documentado; gestão de vulnerabilidades com ciclo de atualização definido; proteção de dados sensíveis com criptografia e segregação; capacitação de servidores para reconhecer ameaças; e comunicação transparente com cidadãos em caso de violação.

A Autoridade Nacional de Segurança Cibernética (ANSC), criada em 2024, e as normas do Gabinete de Segurança Institucional sobre cibersegurança

no governo federal são avanços na direção certa. O desafio é que muitos órgãos, especialmente municipais e estaduais de menor porte, não têm capacidade de implementar *frameworks* sofisticados sem apoio técnico, financeiro e normativo da União.

Segurança digital é um bem público que não pode depender apenas da capacidade individual de cada órgão. Exige infraestrutura compartilhada, padrões mínimos obrigatórios, apoio a entes subnacionais e cultura organizacional que trate vulnerabilidade como risco de governança, não como constrangimento técnico a ser ocultado.

A intersecção entre cibersegurança e IA merece atenção específica. Sistemas de inteligência artificial introduzem novos vetores de risco que os *frameworks* de segurança tradicionais não cobrem integralmente: modelos podem ser envenenados em seus dados de treinamento, resultados podem ser manipulados por ataques adversariais, e agentes autônomos podem ser induzidos a tomar decisões prejudiciais por entradas maliciosas. O Financial Stability Board, em suas *12 Sound Practices for Responsible Adoption of AI* (junho de 2026), dedicou uma prática específica à segurança cibernética de sistemas de IA, reconhecendo que gerir o risco de IA exige camadas de proteção distintas das aplicadas a sistemas convencionais. Para o setor público brasileiro, isso significa que a ANSC e os órgãos setoriais com sistemas de IA em produção precisam ir além dos *frameworks* genéricos de cibersegurança e incorporar controles específicos para o ciclo de vida de modelos: proteção do *pipeline* de dados de treinamento, monitoramento contínuo de *drift* e comportamento anômalo, e planos de resposta a incidentes que contemplem a possibilidade de comprometimento do próprio modelo.

Esse risco deixou de ser abstrato quando a própria comunidade de segurança cibernética passou a tratá-lo como categoria própria. Em abril de 2026, seis agências de cinco países, lideradas pela CISA e pela NSA dos Estados Unidos, com Reino Unido, Canadá, Austrália e Nova Zelândia, publicaram o guia *Careful Adoption of Agentic AI Services*, a primeira orientação multinacional coordenada especificamente sobre agentes de IA. O documento organiza os riscos em cinco categorias, escalonamento de privilégios, falhas de projeto e configuração, desalinhamento de comportamento, fragilidade estrutural e lacunas de responsabilização, e fixa uma exigência que a administração pública tende a inverter: cibersegurança é pré-requisito, não etapa posterior. Antes de colocar um agente autônomo para operar sobre sistemas públicos, é preciso limitar privilégios ao mínimo necessário, isolar componentes de terceiros e manter trilha de auditoria de cada ação do agente. Do lado da implementação, o guia de referência do CSET da Universidade de Georgetown, também de 2026, ataca o problema complementar: consolida mais de 1.200 recursos

técnicos num roteiro navegável que traduz princípios de alto nível de governança de IA em práticas concretas ao longo do ciclo de vida, exatamente a camada operacional que falta à maioria dos órgãos brasileiros, presos entre a declaração de princípios e a implantação sem controle.

Há uma medida de quanto essa inversão custa quando não é feita. O relatório anual da IBM com o Ponemon Institute, na edição de 2026, estudou 602 organizações atingidas por violações de dados entre março de 2025 e fevereiro de 2026 e encontrou custo médio global de USD 4,99 milhões por violação, alta de 12% e recorde da série, com detecção, escalonamento e perda de negócio respondendo por 63% do total. Mais de uma em cada quatro organizações atacadas relatou que o ataque era conduzido por IA, crescimento de 56% em um ano, e ataques dessa natureza acrescentaram cerca de USD 1 milhão por violação. Quando o alvo foi o próprio modelo, a inversão de modelo custou em média USD 6,07 milhões e a injeção de prompt, USD 5,89 milhões.

O achado mais relevante para este capítulo não é o custo, é a causa. Entre as organizações que sofreram violação relacionada a IA, 92% não tinham controles de acesso adequados sobre modelos e dados, e apenas 40% do conjunto relatou usar tais controles. Dois terços das organizações violadas, 68%, não tinham governança capaz de gerenciar o uso de IA ou de detectar shadow AI, proporção pior que a do ano anterior. E a exigência de aprovação formal para implantar IA, o controle de governança mais comum, caiu de 45% para 38%. Ou seja: no mesmo período, a adoção acelerou e a supervisão recuou. Cabe a ressalva metodológica de que o estudo é patrocinado por fornecedor de tecnologia de segurança e sua amostra é majoritariamente privada, o que recomenda tratá-lo como evidência de tendência corporativa e não como estatística do setor público. Ainda assim, a direção do achado é exatamente a tese deste capítulo, agora com número: a entrega tecnológica cresce mais rápido que a capacidade de governá-la.

Na direção oposta, convém resistir à tentação de calibrar política pública pelo cenário mais dramático disponível. Um estudo de Matthew van der Merwe para o Centre for the Governance of AI, de 2026, avaliou se sistemas de IA poderiam habilitar um ciberataque catastrófico à rede elétrica dos Estados Unidos, com dano da ordem de USD 100 bilhões, equivalente a deixar cerca de cem milhões de pessoas sem energia por aproximadamente uma semana. A conclusão é cautelosa e útil: o gargalo principal não parece ser um obstáculo técnico único, e sim a capacidade operacional de coordenar muitas capacidades contra dezenas ou centenas de alvos simultâneos. O autor sugere que ataques de menor magnitude oferecem limiares mais úteis para avaliação de risco e desenho de mitigação.

A implicação é de método. Cenário extremo é bom modelo de risco e mau gatilho de política, porque justifica investimento caro e específico contra o evento menos provável, enquanto o dano recorrente ocorre alguns degraus abaixo. Para o setor público brasileiro, isso significa dimensionar a resposta pelo incidente que efetivamente acontece, ataque a hospital municipal, a tribunal, a prefeitura, e não pelo apagão continental que serve melhor à retórica do que ao orçamento.

Um documento de doutrina de cibersegurança nacional produzido em 2026 por um grupo de trabalho estoniano que reúne governo, setor privado e academia oferece um deslocamento conceitual útil para esse debate. Sua premissa é que a IA inverteu a economia do conflito cibernético: atacar ficou mais barato, mais rápido e mais escalável, enquanto o defensor continua obrigado a ser legal, confiável e correto. A resposta a esse desequilíbrio não pode ser gastar na mesma proporção que o adversário, precisa ser assimétrica. O objetivo realista não é a invulnerabilidade. É tornar os incidentes não decisivos: impedir que incidentes virem crises e que crises virem paralisia institucional. O documento parte de uma inversão que interessa diretamente à administração pública brasileira: numa campanha contra um Estado democrático, o dano técnico costuma ser o meio, e a erosão da confiança pública é o fim. Por isso a doutrina trata transparência como instrumento de defesa, não como risco reputacional a ser administrado pela comunicação institucional. A analogia usada é a de um regulador de aviação: a confiança no sistema aéreo não vem da ausência de incidentes, vem de relatórios preliminares publicados em dias e investigações independentes que seguem depois. Um Estado que fala primeiro reduz o espaço para o boato.

Entre as recomendações operacionais do documento estão o dever legal de divulgar incidentes materiais em vinte e quatro horas, um canal oficial por órgão ensaiado antes de cada ciclo eleitoral, e um log de acesso a dados pessoais visível ao próprio cidadão, mostrando quem no Estado consultou seus dados, quando e sob qual base legal. Vale registrar, para não transformar aspiração em conquista já realizada: a Estônia tem esse log, o Andmeajälgi, integrado ao portal eesti.ee, mas hoje ele é voluntário e cobre apenas cerca de quinze dos mais de trezentos sistemas de informação do Estado; o próprio Ministério da Justiça e Assuntos Digitais estoniano, coautor do documento, defende torná-lo obrigatório. O documento cita ainda Taiwan como referência operacional de resposta a desinformação: ministérios publicam esclarecimento assinado logo após o surgimento de um boato sob a chamada regra 2-2-2, desmentido em vinte minutos, duzentas palavras, duas imagens, com o lema humor sobre boato. A disciplina é medida em tempo e alcance, não em volume de comunicação.

Para o Brasil, a lição não é replicar cada recomendação estoniana literalmente. É reconhecer que a mesma arquitetura de accountability defendida neste livro para integridade e compras públicas tem, também, fundamento de segurança nacional: transparência ativa e auditável não é custo de conformidade. É infraestrutura defensiva.

6. OBJETIVOS DIGITAIS: METAS ANTES DE TECNOLOGIA

Os *Digital Development Goals* para cidades partem de uma percepção correta: a transformação digital urbana avançou tanto que os marcos tradicionais de desenvolvimento não capturam completamente seus desafios. Cidades estão digitalizando infraestrutura, serviços, mobilidade, segurança, participação, planejamento e interação com cidadãos. IA, *digital twins*, sensores e plataformas urbanas ampliam possibilidades e riscos.

Mas uma agenda de objetivos digitais pode cair em duas armadilhas. A primeira é a abstração excessiva: metas genéricas, vocabulário sofisticado, princípios consensuais e baixa utilidade para decisões reais. A segunda é a tecnocratização: indicadores, plataformas e linguagem digital sem governança, inclusão, *accountability* e capacidade institucional.

Um objetivo como inclusão digital urbana não pode ser apenas “aumentar acesso”. Precisa explicitar quais serviços devem ser acessíveis, para quem, com quais barreiras removidas, com quais canais alternativos, com que proteção contra exclusão e com que métrica de uso efetivo. Um objetivo de governança de IA urbana não pode ser apenas “usar IA de forma responsável”. Precisa exigir dados interoperáveis, *logs*, auditoria, explicabilidade proporcional, regras de contestação e responsabilização.

Metas digitais sem capacidade institucional viram poesia administrativa.

Há ainda uma dimensão de sustentabilidade que a agenda de objetivos digitais precisa incorporar com mais seriedade. Transformação digital tem impactos materiais frequentemente invisibilizados. *Data centers* consomem quantidades expressivas de energia e água. Equipamentos eletrônicos têm ciclo de vida limitado e produzem resíduos de difícil gestão. IA de alta escala demanda infraestrutura computacional intensiva. A narrativa de que digital é necessariamente mais sustentável do que analógico não se sustenta em todos os contextos e para todas as escalas. Uma agenda digital séria precisa avaliar *trade-offs* de sustentabilidade como critério de escolha tecnológica, não apenas como narrativa de comunicação.

7. MÉTRICAS QUE MUDAM GESTÃO

A experiência do *Balanced Scorecard* na Anatel oferece uma lição que permanece atual: ferramenta de gestão só cria valor quando se conecta a rotina, responsabilidade e decisão.

O BSC traduzia estratégia em objetivos, indicadores, metas e projetos. Mas seus desafios não estavam apenas no desenho inicial. Estavam na continuidade: acompanhamento sistemático, atualização das informações, governança de projetos, alinhamento organizacional e disciplina de gestão.

Essa lição vale integralmente para transformação digital.

Painéis digitais são fáceis de celebrar e difíceis de institucionalizar. Podem dar visibilidade, organizar informação e apoiar coordenação. Mas, sem reunião de gestão, responsável pelo indicador, regra de escalonamento e consequência, o painel vira decoração administrativa. O número muda; a organização não.

Uma métrica digital útil precisa responder a quatro perguntas: que decisão ela informa? Quem a acompanha? Com que frequência? O que acontece quando ela cruza determinado limite?

Se a resposta não for clara, a métrica provavelmente serve mais à apresentação do que à gestão.

Isso é particularmente relevante nas agendas de cidades digitais, DPI e objetivos digitais de desenvolvimento. Medir o número de serviços digitalizados pode ser útil, mas é insuficiente. É preciso medir acesso efetivo, uso por grupos vulneráveis, tempo de resolução, redução de deslocamentos, satisfação, contestação, falhas, incidentes, custos, interoperabilidade real, segurança, impacto sobre servidores e efeitos distributivos.

Da mesma forma, medir adoção de IA não demonstra maturidade. Um órgão pode ter muitos casos de uso e pouca governança. Pode automatizar tarefas irrelevantes e deixar decisões críticas sem melhoria. Pode aumentar produtividade aparente e reduzir qualidade decisória. Capacidade estatal digital exige métricas com consequência.

Um painel com conselheiros e diretores de segurança da informação de grandes empresas, reunido pela McKinsey e pela National Association of Corporate Directors em 2026, chegou a um diagnóstico equivalente para o setor privado, e a semelhança com a administração pública é direta: o modelo tradicional de supervisão de risco, com revisão trimestral em formato de heat map, não captura um risco que muda diariamente. Um dos participantes do painel, Guy Gecht, resumiu a virada de forma direta: depois de décadas protegendo dados, as organizações agora precisam proteger julgamento, porque sistemas

de IA cada vez mais recomendam decisões a humanos, e o ponto de falha se deslocou do dado para a decisão informada por ele. O paralelo com a gestão pública é exato: um painel de indicadores revisado uma vez por trimestre é a versão administrativa do heat map trimestral, e sofre da mesma limitação diante de sistemas cujo comportamento pode mudar em dias.

O que distingue uma cultura de gestão digital madura de uma cultura de entrega digital performática é a disposição de medir o que incomoda. Taxa de falha de autenticação que exclui cidadãos vulneráveis. Percentual de casos que retornam ao atendimento presencial após interação digital. Tempo médio entre identificação de vulnerabilidade de segurança e aplicação de *patch*. Proporção de alertas de risco que resultaram em ação versus proporção que foram ignorados. Número de contestações de decisões automatizadas acolhidas versus rejeitadas. Esses são indicadores que revelam a qualidade real do sistema digital, e que poucos órgãos medem sistematicamente, justamente porque o resultado pode ser constrangedor.

8. COMPRAS PÚBLICAS E DEPENDÊNCIA TECNOLÓGICA

Grande parte da transformação digital pública passa por compras públicas. Sistemas, nuvem, consultorias, licenças, modelos, sensores, plataformas, equipamentos, manutenção e serviços especializados dependem de contratações.

Isso torna compras públicas parte da política digital, não apenas uma etapa administrativa.

Se o Estado compra mal, digitaliza mal. Contratos podem criar dependência de fornecedor, dificultar interoperabilidade, restringir acesso a dados, impedir auditoria, elevar custos de mudança e tornar a administração refém de soluções proprietárias. O problema não é contratar o setor privado. O problema é contratar sem arquitetura, sem padrões e sem estratégia de longo prazo.

Uma agenda séria de capacidade digital precisa incorporar, nos processos de compra, requisitos de portabilidade, documentação, APIs abertas, segurança, *logs*, continuidade, governança de dados, acessibilidade, sustentabilidade e possibilidade de auditoria. É preciso também avaliar custo total de propriedade, não apenas preço inicial. Um sistema barato que aprisiona dados, exige manutenção cara ou impede integração pode sair muito mais caro para o Estado ao longo do tempo.

A concentração do mercado de tecnologia é, igualmente, uma questão de governança pública. Poucos fornecedores dominam segmentos críticos como nuvem, sistemas de gestão, soluções de IA e infraestrutura de segurança. Quando um órgão migra completamente para um fornecedor sem prever

saída, cria dependência que vai além do contrato: pode significar que dados públicos só estão acessíveis mediante pagamento contínuo a um ator privado. Soberania de dados é questão estratégica, não apenas técnica.

A experiência europeia recente ilustra o limite dessa estratégia quando ela para na regulação. Um relatório do IE University (Centro para a Governança da Mudança), de fevereiro de 2026, sobre a geopolítica da revolução digital argumenta que a União Europeia projetou normas globais de peso, o GDPR, o Digital Services Act, o Digital Markets Act, o AI Act, mas segue dependente de partes críticas do próprio stack tecnológico que essas normas regulam: nuvem, semicondutores, modelos de fronteira. Poder regulatório sem capacidade material sobre a infraestrutura que se regula produz um tipo específico de vulnerabilidade: o regulador define as regras, mas não controla os meios de produção da tecnologia regulada. Para o Brasil, que não tem sequer o poder regulatório consolidado que a Europa já tem, a lição chega adiantada: regular compras de tecnologia, exigir portabilidade e auditabilidade em contrato é necessário, mas não substitui a pergunta mais difícil, que capacidades tecnológicas críticas o país precisa deter para não regular apenas o que outros construíram.

A Nova Lei de Licitações e Contratos (Lei 14.133/2021) trouxe avanços relevantes para compras de tecnologia: contratação por bandas de desempenho, maior flexibilidade para serviços de TI, critérios de inovação e a figura do diálogo competitivo para objetos complexos. Mas nenhuma inovação normativa substitui a capacidade técnica de quem contrata. Um edital bem escrito por uma equipe que não compreende o que está comprando ainda pode gerar dependência. A competência de contratar tecnologia, entender requisitos funcionais, avaliar propostas técnicas, negociar cláusulas de dados e portabilidade, monitorar contratos e medir entrega, é uma capacidade institucional que precisa ser desenvolvida sistematicamente.

Boas práticas de contratação de tecnologia incluem: especificação por resultado público esperado, não por solução técnica específica; exigência de código aberto ou, no mínimo, de acesso completo aos dados em formatos padrão; cláusulas de auditabilidade que permitam ao órgão verificar o funcionamento do sistema; obrigações de documentação e transferência de conhecimento ao final do contrato; vedação de cláusulas que restrinjam a capacidade do órgão de trocar de fornecedor; e avaliação de desempenho com métricas definidas antes da contratação, não após a entrega.

9. CAPACIDADE LOCAL E DESIGUALDADE DIGITAL

Nenhuma agenda digital nacional ou global funcionará se ignorar a desigualdade de capacidade entre territórios.