EBOOK ESTRATÉGICO · ALTA GESTÃO

PARA MINISTROS, SECRETÁRIOS, CIOS DO GOVERNO, COMANDANTES MILITARES, DIRIGENTES DE AGÊNCIAS DE INTELIGÊNCIA E CONSELHOS DE EMPRESAS ESTATAIS

A Soberania *Calculável*.

Como a Criptografia Totalmente Homomórfica permite ao Estado cruzar bases de dados, treinar IA, conduzir vigilância legítima e operar inteligência — sem expor cidadão e sem entregar soberania a fornecedores estrangeiros.

VOLUME I · EDIÇÃO 2026 · CONFIDENCIAL

SUMÁRIO

O que você vai *ler*.

- Apêndices

O argumento em *uma* página.

Se você só vai ler uma coisa deste eBook, leia isto.

O Estado brasileiro é, hoje, o maior detentor de dado pessoal sensível do país — e talvez o operador menos eficiente desse acervo. Receita Federal, INSS, SUS, Justiça Eleitoral, Polícia Federal, ABIN, Forças Armadas, IBGE, Detrans estaduais, Cadastros Únicos, sistemas de educação. Cada uma dessas operações acumula dados de milhões de cidadãos, em volume e granularidade que nenhum ator privado consegue replicar. E quase todos esses acervos estão paralisados por silos institucionais, incompatibilidade técnica, desconfiança entre órgãos, e — especialmente — pela ausência de uma arquitetura técnica que permita cruzamento legítimo sem violar a privacidade do cidadão.

O resultado é uma situação simultaneamente trágica e absurda. Trágica porque o Estado tem dado para resolver problemas sociais reais (focalização de programas sociais, detecção de fraude previdenciária, identificação precoce de riscos epidemiológicos, combate à evasão fiscal, segurança pública baseada em evidência) e não consegue usar. Absurda porque muito desse dado, quando finalmente cruzado, é cruzado em condições piores do que se fosse processado tecnicamente — via planilhas trocadas em pendrives, sistemas integrados de forma frágil, fornecedores terceirizados que não respondem ao Estado.

1

SILOS POR DESENHO

Constituição e LGPD limitam corretamente o cruzamento sem base legal. Mas a arquitetura técnica não evoluiu para tornar cruzamento legítimo viável.

2

CLOUD ESTRANGEIRA

Boa parte da operação digital do governo brasileiro roda em AWS, Azure, GCP — fornecedores sujeitos a CLOUD Act americano.

3

4

CRQC CHEGANDO

Computador quântico criptograficamente relevante estimado para 2029. Toda a criptografia atual de governo será quebrada.

IA TERCEIRIZADA

Governo cada vez mais usa LLMs estrangeiras. Cada decisão pública mediada por modelo de outra nação é entrega de soberania.

FHE — Criptografia Totalmente Homomórfica — é a tecnologia que destrava as quatro frentes simultaneamente. Permite cruzamento entre agências sob garantia matemática de minimização. Permite usar cloud estrangeira sem entregar dado em claro. Posiciona o Estado para a transição pós-quântica. E permite operar IA soberana sem depender de modelos estrangeiros sobre dados de cidadãos.

> *"A próxima década do Estado digital será definida por quais nações souberem operar dado de cidadão sem perder soberania para fornecedores, e sem trair a privacidade que a Constituição garante."*

A DECISÃO

Não é uma decisão técnica. É uma decisão de soberania nacional. O Estado que não dominar computação privada será, em cinco anos, dependente operacional de fornecedores estrangeiros para tudo o que importa.

CAPÍTULO I

O Estado como *Cofre Distribuído*.

O setor público brasileiro é o maior detentor de dado do país. E o ator mais paralisado quando se trata de transformar esse dado em capacidade.

Toda agência pública brasileira que opera em escala nacional acumula dados de milhões de cidadãos. Receita Federal tem declarações de imposto, movimentação bancária, operação de cartão de crédito reportada. INSS tem contribuição, vínculo trabalhista, histórico de benefício. SUS tem prontuário ambulatorial, dispensação, internação, vacinação. Justiça Eleitoral tem cadastro eleitoral, biometria, geolocalização de votação. Polícia Federal tem antecedentes, mandados, viagens internacionais. ABIN tem inteligência classificada. Forças Armadas têm dados operacionais. IBGE tem censo demográfico, social, econômico. Cada um desses acervos é uma janela parcial sobre o cidadão. Combinados, formam uma imagem inteira — e perigosamente concentrada.

A regulação brasileira (LGPD + Constituição + jurisprudência sobre direito à privacidade) limita corretamente o cruzamento dessas bases sem base legal específica. O resultado é que cada agência opera sobre seu próprio silo, raramente cruza com outras, e quando cruza o faz através de mecanismos frágeis — convênios, planilhas, integrações pontuais, sistemas de "consulta" que precisam ser autorizados caso a caso.

O paradoxo do dado público

O Estado tem o dado mais valioso do país e a maior dificuldade institucional em usá-lo legitimamente. Cada projeto de cruzamento entre agências exige autorização específica, parecer jurídico, debate público, frequentemente lei específica. O custo institucional de qualquer iniciativa nova é tão alto que muitas iniciativas valiosas simplesmente não acontecem.

Os ativos invisíveis do Estado

ATIVO	O QUE É	POR QUE ESTÁ PARALISADO
Receita	Declaração + movimentação financeira	Sigilo fiscal absoluto
SUS	Prontuário ambulatorial nacional	Categoria especial LGPD
Cadastro Único	Vulnerabilidade social	Cruzamento bloqueado por lei
INSS	Contribuição e benefício	Sigilo previdenciário
Eleitoral	Cadastro biométrico	Sigilo do voto
Defesa	Operacional militar	Sigilo de segurança nacional
Inteligência	ABIN, Coaf	Compartimentação institucional

O que mudou na cadeia de valor

O que mudou nos últimos dez anos é que o Estado começou a investir pesado em transformação digital — sem investir em arquitetura criptográfica equivalente. Cloud-first, integração via API, IA aplicada, cidadão digital. Cada uma dessas iniciativas é boa isoladamente. Combinadas, criaram uma operação de dado em escala que nunca foi acompanhada por evolução criptográfica.

O Estado brasileiro hoje processa dado de milhões de cidadãos em data centers próprios e em cloud estrangeira, com criptografia tradicional, sob arquitetura que foi desenhada para um mundo que assume confiança em fornecedores. Esse mundo está mudando, e a transição precisa ser conduzida agora.

O PROBLEMA SILENCIOSO

Boa parte da operação digital do governo brasileiro depende de cloud estrangeira sujeita a CLOUD Act americano. Isto significa que dado de cidadão brasileiro pode, em princípio, ser acessado por governo estrangeiro mediante ordem judicial daquele governo. A LGPD e a Constituição brasileira protegem em tese; a arquitetura técnica não protege na prática.

“A pergunta para o dirigente público não é se a arquitetura atual de dado é sustentável. É quanto soberania o Brasil já entregou sem decretar, e quanto tempo falta até essa entrega virar problema concreto.”

CAPÍTULO II

O Cerco *Geopolítico*.

A regulação que governa o Estado é simultaneamente a mais robusta (Constituição) e a mais subexplorada tecnicamente. As pressões externas estão aumentando.

LGPD aplicada ao próprio Estado

A LGPD se aplica ao Estado, mas com regime próprio. O artigo 23 determina que tratamento de dado pessoal por pessoa jurídica de direito público deve ser para finalidade pública, com base legal específica. A ANPD tem demonstrado disposição em fiscalizar o próprio Estado — em 2023 e 2024 emitiu recomendações contra ministérios por excesso de tratamento.

CLOUD Act e a perda silenciosa de soberania

O CLOUD Act americano (2018) permite ao governo dos EUA exigir dados de empresas americanas — incluindo dados armazenados fora dos EUA. Isto significa que AWS, Azure, GCP e outras provedoras americanas que hospedam dados brasileiros estão, em princípio, sujeitas a ordens judiciais americanas. A LGPD e a Constituição brasileira oferecem proteção formal, mas a proteção técnica é frágil. **Cada gigabyte de dado de cidadão brasileiro em cloud americana é potencialmente acessível por governo estrangeiro.**

EHDS, EUDI Wallet e o padrão europeu emergente

A Europa está construindo o European Health Data Space e a EUDI Wallet. Ambos exigirão capacidade técnica de privacy-preserving analytics. Países que quiserem participar de iniciativas europeias precisarão de capacidade equivalente. Isto cria um padrão internacional emergente que o Brasil pode liderar (e ganhar voz) ou seguir (e perder relevância).

CRQC e a obsolescência da criptografia atual

Computador quântico criptograficamente relevante estimado para 2029. Quando vier, quebra ECDSA, RSA, ECDH — toda a criptografia que protege a operação digital do Estado brasileiro hoje. Países sérios já começaram a planejar migração: NSA emitiu CNSA 2.0; UK NCSC publicou diretrizes; França tem ANSSI orientando migração. **O Brasil ainda não tem plano formal nacional de migração pós-quântica.** Isto é um problema de soberania tão urgente quanto qualquer outro.

Adversários sofisticados e HNDL

"Harvest Now, Decrypt Later" — adversários estados-nação estão coletando ciphertext brasileiro hoje, esperando o CRQC chegar para decifrar. Cada documento sigiloso, cada comunicação diplomática, cada operação de inteligência cifrada com criptografia clássica gerada hoje é potencialmente vulnerável retroativamente em 2029-2030.

O custo de não agir

RISCO	PROBABILIDADE 5 ANOS	IMPACTO
Vazamento retroativo pós-CRQC de comunicação sensível	Alta após 2029	Catastrófico — décadas de inteligência exposta
Acesso de governo estrangeiro a dado brasileiro via CLOUD Act	Já ocorre	Perda de soberania não declarada
Multa LGPD por uso secundário sem base legal	Média	Reputação institucional
Exclusão de iniciativas internacionais por incapacidade técnica	Alta	Perda de voz em governança global
Dependência de IA estrangeira em decisões públicas	Crescente	Perda de soberania algorítmica

CAPÍTULO III

FHE em Linguagem *Executiva*.

Sem matemática. O que dirigentes públicos precisam entender.

Cofre transparente. Você vê que há algo dentro, não vê o que é. Manipula o conteúdo de fora — soma, multiplica, compara, computa modelos inteiros — sem nunca abrir. Devolve fechado. Apenas o dono da chave abre. Isto é FHE.

Por que é central para soberania

FHE é a única tecnologia que permite executar computação sobre dado em servidor que você não controla, sem que esse servidor tenha acesso ao dado. **Isto reverte a equação atual da computação em nuvem.** Hoje, usar cloud estrangeira significa entregar dado em claro a um fornecedor estrangeiro. Sob FHE, é possível usar cloud estrangeira (mais barata, mais escalável) *sem entregar nada*. O dado entra cifrado, é processado cifrado, sai cifrado. O fornecedor americano nunca tem acesso, mesmo sob ordem do CLOUD Act — porque tecnicamente não tem o dado.

FHE e a transição pós-quântica

Os esquemas modernos de FHE são construídos sobre o problema RLWE — exatamente o mesmo problema sobre o qual NIST padronizou ML-KEM e ML-DSA, a próxima geração de criptografia pós-quântica. **Adotar FHE é adotar PQC implicitamente.** O time que aprende FHE aprende a base da criptografia pós-quântica. A infraestrutura que suporta FHE suporta PQC.

Como funciona

> **ANALOGIA PARA O SETOR PÚBLICO**
>
> Receita cifra sua base com chave própria. INSS cifra a sua. Ambas enviam para um servidor neutro (ou cloud) que executa o cruzamento sob cifra. Devolve apenas a estatística agregada cifrada. Apenas o agregador autorizado (com chave threshold) decifra o resultado final. Em nenhum momento o servidor — americano, brasileiro, ou qualquer outro — viu dado individual em claro.

FHE vs alternativas

TECNOLOGIA	PROMETE	FALHA
Anonimização	"Removemos identificadores"	Re-identificação trivial; já invalidada
TEE	"O chip isola"	Confia no fabricante (estrangeiro!)
Federated Learning	"Dado fica local"	Gradientes vazam dado
Differential Privacy	"Adicionamos ruído"	Inadequado para decisão individual
FHE	**"Servidor nunca vê em claro"**	**Custo computacional alto — mas decrescente**

Para o setor público, a vantagem de FHE sobre TEE é especialmente importante: TEE depende de confiar no fabricante estrangeiro do chip (Intel, AMD). **FHE não depende de confiar em ninguém.**

CAPÍTULO IV

Casos de Uso por *Área*.

Cruzamento entre agências sob garantia matemática

Este é o caso âncora. Receita quer cruzar com INSS para detectar fraude previdenciária. Polícia Federal quer cruzar com Receita para investigação de lavagem. SUS quer cruzar com Cadastro Único para focalização de programa social. Cada um desses cruzamentos é juridicamente possível em casos específicos, mas tecnicamente complexo, demorado, e politicamente caro.

Sob FHE: cada agência cifra sua base. Cruzamento acontece sobre cifras. O resultado decifrado é apenas a estatística ou o subconjunto autorizado por base legal específica. Nenhuma agência vê a base inteira da outra. **Isto destrava cruzamentos legítimos sem violar privacidade nem soberania institucional.**

Cloud estrangeira sem entregar soberania

Boa parte da operação digital do governo brasileiro roda em AWS, Azure, GCP. Migrar tudo para cloud nacional seria caro e impraticável. Sob FHE, é possível continuar usando cloud estrangeira *com dado cifrado*. O cloud provider hospeda, processa, escala — mas nunca tem acesso ao plaintext. **O CLOUD Act perde força** porque tecnicamente o provedor americano não tem o dado, mesmo se ordenado a entregar.

Censo e estatística pública sob privacidade

O IBGE conduz censos, PNAD, pesquisas. Cada uma envolve dado de milhões de domicílios, com obrigação constitucional de sigilo. Atualmente, esse dado é processado por equipes do IBGE com acesso direto. Sob FHE, o processamento estatístico pode acontecer sobre dados cifrados, e nem mesmo os técnicos do IBGE precisam ver dado individual. Isto eleva a confiança pública na estatística oficial e abre possibilidades de divulgação pública mais granular sem risco de re-identificação.

Eleição verificável e auditoria do voto

O Brasil tem uma das eleições eletrônicas mais avançadas do mundo — e uma das mais auditáveis. FHE pode adicionar uma camada nova: **contagem matematicamente verificável sem expor o voto individual**. Junto com provas de conhecimento zero (ZKP), permite auditoria pública de cada urna sem que ninguém — nem o TSE — consiga associar voto a eleitor. Isto fortalece a legitimidade da eleição contra qualquer questionamento futuro.

Inteligência e segurança nacional

Operações de inteligência exigem cruzamento entre fontes (sinais, humana, financeira, geo). Cada fonte é compartimentada por razão de segurança. FHE permite cruzar fontes sem que nenhuma compartimentação seja quebrada — analistas autorizados acessam apenas o resultado combinado, nunca a fonte individual. Isto é especialmente útil em colaboração internacional de inteligência, onde compartilhamento de fonte primária é vetado.

Defesa e operações militares

Forças Armadas operam dados de inteligência operacional, logística, pessoal, missão. A migração para PQC é prioridade explícita de qualquer doutrina militar séria — adversários sofisticados estão fazendo HNDL contra comunicações militares brasileiras hoje. FHE oferece um caminho duplo: capacidade colaborativa (entre forças, entre aliados) e migração estruturada para PQC.

IA soberana sobre dado público

O Estado brasileiro está usando cada vez mais LLMs e modelos de visão estrangeiros para processar documentos, classificar pedidos, gerar respostas a cidadãos. Cada uso é uma entrega de soberania algorítmica. Sob FHE, o Estado pode usar modelos estrangeiros sem entregar dado — ou, melhor ainda, treinar modelos próprios sobre dado de cidadão sem expor o dado.

Cadastro Único e focalização de programa social

Bolsa Família, BPC, programas estaduais. Toda focalização eficaz exige cruzamento entre Cadastro Único, INSS, Receita, SUS, e bases estaduais. Hoje esse cruzamento é parcial e atrasado. Sob FHE,

cruzamento contínuo é possível sem violar privacidade. Resultado: **focalização melhor, menos fraude, menos exclusão indevida**.

Saúde pública e vigilância epidemiológica

SUS tem dado epidemiológico em volume e granularidade que poucos países têm. Combinado com dados de farmácia, lab, hospital — permitiria detecção precoce de surto, estudo de eficácia real de tratamento, vigilância farmacovigilância. Sob FHE, essas combinações são possíveis sem comprometer privacidade individual.

Receita Federal e detecção de evasão

Cruzamento de declaração com movimentação bancária, cartão, importação, e operação imobiliária é o coração da fiscalização tributária. Hoje exige operações específicas autorizadas. Sob FHE, é possível operar continuamente, sob auditoria matemática verificável.

Diplomacia e comunicação confidencial

Comunicações diplomáticas brasileiras hoje usam criptografia clássica vulnerável a CRQC. Migração para PQC é prioridade. FHE adiciona camada extra: permite computação colaborativa com aliados sem expor fonte primária.

CAPÍTULO V

A Economia do *Estado que Calcula sem Ver*.

Capex inicial

COMPONENTE	INVESTIMENTO
Time fundador (cripto sênior, ML, jurídico, gestores de projeto)	R$ 6M – 10M / ano
Licenças e tooling	R$ 400k – 1.5M
Infra computacional soberana	R$ 5M – 15M
Consultoria estratégica	R$ 1.5M – 4M
Estudo regulatório e constitucional	R$ 800k – 2M
Integração com sistemas legados de múltiplas agências	R$ 5M – 15M
Total ano 1	**R$ 19M – 47M**

Opex anual

ITEM	ESTIMATIVA
Compute	R$ 4M – 12M
Time de manutenção	R$ 6M – 12M
Auditoria	R$ 1M – 3M
Opex anual	**R$ 11M – 27M**

Para o governo federal brasileiro com orçamento de TI da ordem de R$ 10-15 bilhões anuais, isto representa **menos de 0,3%**. Para uma agência específica de grande porte, é absorvível.

O retorno — seis vetores

1. Detecção de fraude previdenciária e fiscal

Fraude estimada do INSS: R$ 5-15B anuais. Da Receita: R$ 100-300B anuais (gap tributário). Captura via cruzamento sob FHE: **R$ 5-50B anuais em recuperação**.

2. Focalização de programas sociais

Bolsa Família, BPC e demais têm taxa de erro de inclusão estimada em 5-10%. Redução: **R$ 2-8B anuais**.

3. Soberania digital — proteção contra CLOUD Act

Difícil de quantificar, mas estratégico. Proteção contra acesso estrangeiro a dado de cidadão brasileiro vale capital político e moral.

4. Migração PQC sem retrabalho

Custo estimado de migração emergencial pós-CRQC: **R$ 1-5B**. Migração ordenada a partir de FHE: fração disso.

5. Eleição verificável publicamente

Reduz custo político de qualquer questionamento. Difícil de quantificar mas decisivo para legitimidade democrática.

6. Vantagem em diplomacia e governança global

Brasil que lidera em soberania digital ganha voz em fóruns internacionais. Preço incalculável.

Caso de negócio

~R$ 30M INVESTIMENTO ANO 1	~R$ 18M OPEX ANUAL ESTABILIZADO
R$ 10B+ VALOR HABILITADO EM 5 ANOS	100×+ ROI ESPERADO

> *Para o Estado brasileiro, FHE não é projeto de TI. É infraestrutura crítica de soberania nacional.*

CAPÍTULO VI

Vantagem Competitiva *Geopolítica*.

A geopolítica do século XXI vai ser decidida em três frentes: energia, dado, e capacidade computacional. O Estado que dominar as três terá soberania real. O que perder qualquer uma delas terá soberania parcial. O Brasil tem boa posição em energia. Em dado, está parcialmente bem (volume) e parcialmente mal (capacidade técnica). Em capacidade computacional, depende criticamente de fornecedores estrangeiros.

Os três posicionamentos possíveis

1 — A República Soberana

Foco em independência tecnológica de fornecedores estrangeiros. FHE como infraestrutura para usar cloud estrangeira sem entregar soberania. Plano nacional explícito de migração PQC. Funciona como política de Estado.

2 — O Líder Latino-Americano

Foco em construir consórcio regional (LATAM) de privacy-preserving compute para colaboração intergovernamental. Brasil como articulador. Funciona para política externa.

3 — O Modelo de Estado Digital

Foco em virar referência global de Estado digital com privacidade verificável. Apresentar arquitetura em fóruns internacionais (ONU, OEA, Mercosul). Funciona para construir soft power.

O custo de não posicionar

O cenário a explicitar: o que acontece se o Brasil não adotar FHE estruturalmente nos próximos 36 meses? Resposta: **continua dependente de fornecedores estrangeiros para infraestrutura crítica**,

perde voz em iniciativas internacionais sobre governança de dado, chega despreparado ao CRQC em 2029, e descobre tarde demais que entregou soberania algorítmica para Big Tech.

CAPÍTULO VII

Roadmap de *24 Meses*.

01

MESES 1–6 · APRENDER

Fundação institucional

Constituir grupo de trabalho interministerial. Contratar talento (parceria com universidades públicas: USP, Unicamp, UFRJ, IMPA). Identificar três casos de uso candidatos. Alinhar com ANPD, AGU, GSI.

02

MESES 7–14 · CONSTRUIR

Piloto interagências

Construir um caso ponta a ponta. Recomendação: cruzamento Receita-INSS sob FHE para detecção de fraude previdenciária. Validar latência, governança de chave, rastreabilidade.

03

MESES 15–20 · PRIMEIRA OPERAÇÃO REAL

Operação real com base legal

Lançar o primeiro cruzamento real em produção, com base legal específica e respaldo da AGU. Começar diálogo formal com STF sobre arquitetura.

04

MESES 21–24 · CAPACIDADE NACIONAL

Adoção como infraestrutura crítica

Múltiplos casos. Plano nacional formal. Apresentação em fóruns internacionais. Possível anúncio público de plano de soberania digital.

CAPÍTULO VIII

Riscos, Mitigações e *Armadilhas*.

1 · Resistência institucional entre agências

Alta probabilidade. Cada agência defende seu silo. **Mitigação:** patrocínio do mais alto nível (Casa Civil, Presidência). Sem isso, projeto morre.

2 · Não conseguir contratar talento

Salário público é incompatível com mercado. **Mitigação:** parceria com universidades públicas. Cessão temporária de pesquisadores. Modelo de centro de excelência.

3 · Resistência de fornecedores estrangeiros

AWS, Azure, GCP não vão facilitar a transição. **Mitigação:** negociar como cliente premium. FHE não exige sair da cloud — exige usar de forma diferente.

4 · Incompreensão jurídica

STF, AGU, MP podem interpretar mal a arquitetura. **Mitigação:** educar formalmente. Apresentar pareceres acadêmicos.

5 · Custo computacional para volume nacional

Mitigação: arquitetura híbrida. FHE só onde faz diferença.

Armadilha 1 · Tratar como projeto de TI

FHE deve reportar ao mais alto nível (Casa Civil, Presidência), não a CIO de ministério.

Armadilha 2 · Subestimar a dimensão geopolítica

Esta não é decisão de TI. É decisão de soberania.

Armadilha 3 · Esquecer migração PQC

FHE e PQC devem ser tratados como o mesmo programa nacional.

CAPÍTULO IX · MANIFESTO

Uma carta para a próxima década do *Estado brasileiro*.

A república que vocês servem foi construída sobre uma promessa antiga: a de que existe um espaço, em meio à desigualdade do mundo, onde o Estado pode ser instrumento de proteção, justiça e desenvolvimento coletivo. Que o cidadão que confia ao Estado seu dado mais íntimo — sua saúde, sua renda, seu voto, sua identidade — está fazendo um pacto razoável: eu obedeço, você protege; eu contribuo, você não trai.

Esta promessa atravessou décadas. Sobreviveu a ditaduras, redemocratizações, crises econômicas, transformações tecnológicas. Sobreviveu porque era — e em grande parte ainda é — verdadeira. Os cidadãos que pagam imposto, contribuem para a previdência, usam o SUS, votam em eleição, registram filhos, fazem isso, no fundo, por confiança institucional na promessa republicana.

Mas nos últimos quinze anos, sem que ninguém tenha decretado, o ambiente em que o Estado opera mudou completamente. O dado do cidadão deixou de ser arquivo de papel guardado em armário público. Tornou-se petabyte processado em data center, frequentemente em fornecedores estrangeiros, sob criptografia que será obsoleta em poucos anos, mediada por IA cada vez mais terceirizada a empresas cuja sede é em outras nações. Cada decisão técnica isolada foi razoável. O resultado agregado é uma situação que nenhum dirigente público conscientemente desenharia: a soberania digital brasileira foi parcialmente entregue, e quase ninguém percebeu.

É possível voltar atrás. FHE — Criptografia Totalmente Homomórfica — permite ao Estado fazer tudo o que precisa fazer (cruzar bases para detectar fraude, treinar IA para melhorar serviço, usar cloud estrangeira para escalar) **sem entregar soberania**. É possível, com a tecnologia que existe hoje, em 2026, recuperar parte significativa do controle sobre dado de cidadão sem perder eficiência operacional.

O que está em jogo não é uma feature técnica. É a continuidade da promessa republicana em um mundo tecnológico fundamentalmente novo. É a possibilidade de o Estado brasileiro voltar a ser, sem ambiguidade, instrumento de proteção do cidadão — agora com prova matemática verificável, e não com promessa institucional.

> *“Em três anos, alguns Estados vão estar prontos para o século XXI digital. A pergunta é se o Brasil será um deles, ou aquele para quem outros vão olhar como exemplo do que evitar. ”*

Há uma janela. É curta. É real. O resto é coragem política.

APÊNDICE A

Glossário *Executivo*.

FHE

Computação sobre dado cifrado.

RLWE

Base matemática do FHE moderno e do PQC do NIST.

CRQC

Cryptographically Relevant Quantum Computer. Estimativa: 2029.

HNDL

Harvest Now, Decrypt Later — adversários coletam ciphertext hoje.

ML-KEM, ML-DSA

Algoritmos pós-quânticos NIST (FIPS 203, 204).

CLOUD ACT

Lei americana de 2018 que permite ao governo dos EUA exigir dados de empresas americanas, mesmo armazenados fora.

EHDS

European Health Data Space — modelo europeu de uso secundário de dado clínico.

EUDI WALLET

Carteira de identidade digital europeia.

PSI

Private Set Intersection. Caso central para cruzamento entre agências.

THRESHOLD CRYPTOGRAPHY

Distribuição de chave entre múltiplas partes com quórum exigido.

LATTIGO, OPENFHE, CONCRETE

Bibliotecas FHE.

APÊNDICE B

Fornecedores e *Parceiros*.

VENDOR	FOCO
Tune Insight (Suíça/EPFL)	Lattigo, foco em pesquisa colaborativa multi-instituição
Inpher (Suíça/EUA)	FHE+MPC, casos em finanças e governo
Duality (EUA/Israel)	OpenFHE, parceria com NIH
Zama (Paris)	Concrete, TFHE
Stickybit (Brasil)	Boutique técnica brasileira em FHE/PQC — único brasileiro nesta lista

Centros acadêmicos brasileiros

- **USP / IME-USP** — pesquisa em criptografia e segurança
- **Unicamp / IC** — criptografia avançada
- **UFRJ / COPPE** — segurança e sistemas distribuídos
- **IMPA** — matemática de reticulados

APÊNDICE C

30 Perguntas para o *Dirigente Público*.

Estratégia

1. Temos plano nacional de soberania digital?
2. Temos plano de migração pós-quântica?
3. Quanto da nossa operação digital depende de cloud estrangeira?
4. Quanto dado de cidadão está hospedado em fornecedor sujeito a CLOUD Act?
5. Quem responde por isso no organograma?

Casos prioritários

6. Quanto perdemos por ano em fraude previdenciária?
7. Qual o gap tributário evitável?
8. Qual o erro de inclusão em programas sociais?
9. Quais cruzamentos entre agências estão hoje paralisados?
10. Quais pesquisas científicas dependem de dado público hoje inacessível?

Técnica

11. Esquema FHE para o nosso primeiro caso?
12. Latência aceitável?
13. Como integramos com sistemas legados de cada agência?
14. Como gerenciamos chaves entre múltiplas agências?
15. Threshold cryptography compatível?

Custo

16. Custo FHE vs plaintext em volume nacional?
17. Construir interno (universidade pública) ou via consultoria?
18. Capex e opex 24 meses?
19. Sponsor político confirmado?

Regulação

20. Conformidade com LGPD aplicada ao Estado?
21. Parecer da AGU?
22. Diálogo com ANPD?
23. STF entende a arquitetura?
24. Comunicação ao cidadão?

Geopolítica

25. Quanto do nosso dado estrangeiros podem acessar via CLOUD Act?
26. Como protegemos comunicação diplomática de HNDL?
27. Como nos posicionamos em fóruns internacionais sobre governança de dado?
28. Como ganhamos voz em padrões pós-quânticos?
29. Como protegemos defesa nacional?
30. Pior cenário se outras nações chegarem antes?

~

A Soberania Calculável

eBook estratégico para a alta gestão do setor público e soberania digital.
Volume I · Edição 2026 · Distribuição confidencial.

Composto em Iowan Old Style e SF Pro.

— fim —