PT EN

STRATEGIC EBOOK · EXECUTIVE LEVEL

FOR MINISTERS, SECRETARIES, GOVERNMENT CIOS, MILITARY COMMANDERS, INTELLIGENCE AGENCY DIRECTORS AND BOARD MEMBERS OF STATE-OWNED ENTERPRISES

Computable *Sovereignty*.

How Fully Homomorphic Encryption enables the State to cross-reference databases, train AI, conduct lawful surveillance and operate intelligence — without exposing the citizen and without surrendering sovereignty to foreign vendors.

VOLUME I · EDITION 2026 · CONFIDENTIAL

TABLE OF CONTENTS

PT EN

What you will *read*.

Appendices

PT EN

PT EN

The argument in *one* page.

If you read only one thing from this eBook, read this.

The Brazilian State is, today, the country's largest holder of sensitive personal data — and perhaps the least efficient operator of this collection. Federal Revenue Service, Brazilian Social Security (INSS), the Unified Health System (SUS), the Electoral Justice, Federal Police, ABIN intelligence agency, the Armed Forces, Brazilian Statistics Institute (IBGE), state traffic departments, unified social registries, education systems. Each of these operations accumulates data from millions of citizens, in volume and granularity that no private actor can replicate. And nearly all of these collections are paralyzed by institutional silos, technical incompatibility, distrust between agencies, and — especially — the absence of a technical architecture that would allow legitimate cross-referencing without violating citizen privacy.

The result is a situation that is both tragic and absurd. Tragic because the State has the data to solve real social problems (targeting of social programs, detection of social-security fraud, early identification of epidemiological risks, fighting tax evasion, evidence-based public safety) and cannot use it. Absurd because much of that data, when finally cross-referenced, is processed under worse conditions than if handled technically — through spreadsheets exchanged on USB drives, fragile system integrations, third-party vendors who do not answer to the State.

1

SILOS BY DESIGN

The Constitution and LGPD (Brazilian data protection law) rightly limit cross-referencing without legal basis. But the technical architecture has not evolved to make legitimate cross-referencing feasible.

2

FOREIGN CLOUD

Much of the Brazilian government's digital operation runs on AWS, Azure, GCP — providers subject to the U.S. CLOUD Act.

3

4

CRQC APPROACHING

A cryptographically relevant quantum computer is estimated for 2029. All current government encryption will be broken.

OUTSOURCED AI

Government increasingly uses forei
Every public decision mediated by a model from another nation is a surrender of sovereignty.

PT EN

FHE — Fully Homomorphic Encryption — is the technology that unlocks all four fronts simultaneously. It enables cross-agency matching under mathematical guarantees of minimization. It allows using foreign cloud without handing over plaintext data. It positions the State for the post-quantum transition. And it enables operating sovereign AI without depending on foreign models over citizen data.

> *"The next decade of the digital State will be defined by which nations know how to operate citizen data without losing sovereignty to vendors, and without betraying the privacy the Constitution guarantees."*

THE DECISION

This is not a technical decision. It is a decision of national sovereignty. The State that fails to master private computing will be, within five years, operationally dependent on foreign vendors for everything that matters.

CHAPTER I

PT EN

The State as a *Distributed Vault*.

The Brazilian public sector is the country's largest data holder. And the actor most paralyzed when it comes to turning that data into capability.

Every Brazilian public agency operating at national scale accumulates data on millions of citizens. The Federal Revenue Service holds tax returns, bank transactions, reported credit-card activity. Brazilian Social Security (INSS) holds contributions, employment records, benefit history. SUS holds outpatient records, drug dispensing, admissions, vaccinations. The Electoral Justice holds voter registration, biometrics, polling geolocation. Federal Police holds criminal records, warrants, international travel. ABIN holds classified intelligence. The Armed Forces hold operational data. IBGE holds demographic, social and economic censuses. Each of these collections is a partial window on the citizen. Combined, they form an entire image — and a dangerously concentrated one.

Brazilian regulation (LGPD + Constitution + privacy jurisprudence) rightly limits cross-referencing of these bases without specific legal grounds. The result is that each agency operates over its own silo, rarely cross-references with others, and when it does, it does so through fragile mechanisms — cooperation agreements, spreadsheets, one-off integrations, "query" systems that must be authorized case by case.

The paradox of public data

The State holds the country's most valuable data and the greatest institutional difficulty in using it legitimately. Every cross-agency project requires specific authorization, legal opinions, public debate, often specific legislation. The institutional cost of any new initiative is so high that many valuable initiatives simply never happen.

The Invisible Assets of the State

PT EN

ASSET	WHAT IT IS	WHY IT IS PARALYZED
Revenue	Tax returns + financial flows	Absolute tax secrecy
SUS	National outpatient records	LGPD special category
Unified Social Registry	Social vulnerability data	Cross-referencing blocked by law
Brazilian Social Security (INSS)	Contributions and benefits	Social-security secrecy
Electoral	Biometric registry	Voting secrecy
Defense	Military operations	National-security classification
Intelligence	ABIN, Coaf	Institutional compartmentalization

What Changed in the Value Chain

What has changed in the last ten years is that the State began investing heavily in digital transformation — without investing in equivalent cryptographic architecture. Cloud-first, API integration, applied AI, digital citizen services. Each of these initiatives is good in isolation. Combined, they created a data operation at scale that was never matched by cryptographic evolution.

The Brazilian State today processes data on millions of citizens in its own data centers and in foreign clouds, with traditional encryption, under an architecture designed for a world that assumes trust in vendors. That world is changing, and the transition must be led now.

THE SILENT PROBLEM

PT EN

Much of the Brazilian government's digital operation depends on foreign cloud subject to the U.S. CLOUD Act. This means that Brazilian citizen data may, in principle, be accessed by a foreign government under that government's court order. LGPD and the Brazilian Constitution protect in theory; the technical architecture does not protect in practice.

> *"The question for the public leader is not whether the current data architecture is sustainable. It is how much sovereignty Brazil has already surrendered without decreeing it, and how long until that surrender becomes a concrete problem."*

CHAPTER II

PT EN

The Geopolitical *Siege*.

The regulation governing the State is at once the most robust (Constitution) and the most technically underexploited. External pressures are rising.

LGPD applied to the State itself

LGPD (Brazilian data protection law) applies to the State, but under its own regime. Article 23 establishes that processing of personal data by public legal entities must serve a public purpose with specific legal basis. The Brazilian Data Protection Authority (ANPD) has shown willingness to enforce against the State itself — in 2023 and 2024 it issued recommendations against ministries for excessive processing.

CLOUD Act and the silent loss of sovereignty

The U.S. CLOUD Act (2018) allows the U.S. government to compel data from American companies — including data stored outside the U.S. This means that AWS, Azure, GCP and other American providers hosting Brazilian data are, in principle, subject to American judicial orders. LGPD and the Brazilian Constitution offer formal protection, but technical protection is fragile. **Every gigabyte of Brazilian citizen data in an American cloud is potentially accessible by a foreign government.**

EHDS, EUDI Wallet and the emerging European standard

Europe is building the European Health Data Space and the EUDI Wallet. Both will require technical capability for privacy-preserving analytics. Countries that want to participate in European initiatives will need equivalent capability. This creates an emerging international standard that Brazil can lead (and gain voice) or follow (and lose relevance).

CRQC and the obsolescence of current cryptography

A cryptographically relevant quantum computer is estimated for 2029. When it arrives, it breaks ECDSA, RSA, ECDH — all the cryptography that protects the Brazilian State's digital operation today. Serious countries have already begun planning migration: NSA issued CNSA 2.0; UK NCSC published guidance; France has ANSSI directing migration. **Brazil still has no formal national post-quantum migration plan.** This is a sovereignty problem as urgent as any other.

Sophisticated adversaries and HNDL

"Harvest Now, Decrypt Later" — nation-state adversaries are collecting Brazilian ciphertext today, waiting for CRQC to arrive to decrypt it. Every classified document, every diplomatic communication, every intelligence operation encrypted with classical cryptography today is potentially retroactively vulnerable in 2029–2030.

The cost of inaction

PT EN

RISK	PROBABILITY 5 YEARS	IMPACT
Retroactive post-CRQC leak of sensitive communications	High after 2029	Catastrophic — decades of intelligence exposed
Foreign-government access to Brazilian data via CLOUD Act	Already occurring	Undeclared loss of sovereignty
LGPD fine for secondary use without legal basis	Medium	Institutional reputation
Exclusion from international initiatives due to technical incapacity	High	Loss of voice in global governance
Dependence on foreign AI in public decisions	Growing	Loss of algorithmic sovereignty

CHAPTER III

PT EN

FHE in Executive *Language*.

No mathematics. What public leaders need to understand.

Transparent vault. You see there is something inside, you do not see what it is. You manipulate the content from the outside — add, multiply, compare, run entire models — without ever opening it. You return it sealed. Only the key owner opens it. This is FHE.

Why it is central to sovereignty

FHE is the only technology that enables executing computation on data on a server you do not control, without that server having access to the data. **This reverses the current equation of cloud computing.** Today, using foreign cloud means handing over plaintext data to a foreign vendor. Under FHE, it is possible to use foreign cloud (cheaper, more scalable) *without handing over anything*. Data enters encrypted, is processed encrypted, leaves encrypted. The American provider never has access, even under a CLOUD Act order — because technically it does not hold the data.

FHE and the post-quantum transition

Modern FHE schemes are built on the RLWE problem — exactly the same problem on which NIST standardized ML-KEM and ML-DSA, the next generation of post-quantum cryptography. **Adopting FHE means adopting PQC implicitly.** The team that learns FHE learns the foundation of post-quantum cryptography. The infrastructure that supports FHE supports PQC.

How it works

PT EN

> ANALOGY FOR THE PUBLIC SECTOR
>
> The Federal Revenue Service encrypts its database with its own key. Brazilian Social Security (INSS) encrypts its own. Both send to a neutral server (or cloud) that runs the cross-matching under cipher. It returns only the aggregated statistic, still encrypted. Only the authorized aggregator (with a threshold key) decrypts the final result. At no point did the server — American, Brazilian or otherwise — see individual data in plaintext.

FHE vs alternatives

TECHNOLOGY	PROMISES	FAILS
De-identification	"We removed identifiers"	Trivial re-identification; already invalidated
TEE	"The chip isolates"	Trusts the (foreign!) manufacturer
Federated Learning	"Data stays local"	Gradients leak data
Differential Privacy	"We added noise"	Inadequate for individual decisions
FHE	**"Server never sees in plaintext"**	**High computational cost — but decreasing**

For the public sector, FHE's advantage over TEE is especially important: TEE depends on trusting the foreign chip manufacturer (Intel, AMD). **FHE depends on trusting no one.**

CHAPTER IV

PT EN

Use Cases by *Area*.

Cross-agency matching under mathematical guarantees

This is the anchor case. Revenue wants to cross-reference Social Security to detect benefit fraud. Federal Police wants to cross-reference Revenue for money-laundering investigations. SUS wants to cross-reference the Unified Social Registry for social-program targeting. Each of these cross-references is legally possible in specific cases, but technically complex, slow and politically costly.

Under FHE: each agency encrypts its base. Matching happens over ciphertexts. The decrypted result is only the statistic or the subset authorized by specific legal basis. No agency sees the other's full base. **This unlocks legitimate cross-referencing without violating privacy or institutional sovereignty.**

Foreign cloud without surrendering sovereignty

Much of the Brazilian government's digital operation runs on AWS, Azure, GCP. Migrating everything to a national cloud would be expensive and impractical. Under FHE, it is possible to keep using foreign cloud *with encrypted data*. The cloud provider hosts, processes, scales — but never has access to plaintext. **The CLOUD Act loses force** because technically the American provider does not hold the data, even if ordered to hand it over.

Census and public statistics under privacy

IBGE conducts censuses, PNAD, household surveys. Each one involves data from millions of households, with constitutional obligation of secrecy. Currently, this data is processed by IBGE teams with direct access. Under FHE, statistical processing can happen over encrypted data, and not even IBGE technicians need to see individual data. This raises public trust in official statistics and opens possibilities for more granular public disclosure without re-identification risk.

Verifiable elections and vote auditing

Brazil has one of the world's most advanced electronic election systems — and one of the most auditable. FHE can add a new layer: **mathematically verifiable counting without exposing the individual vote**. Together with zero-knowledge proofs (ZKP), it enables public auditing of each ballot box without anyone — not even the Electoral Court — being able to link vote to voter. This strengthens the legitimacy of elections against any future challenge.

Intelligence and national security

Intelligence operations require cross-matching sources (signals, human, financial, geo). Each source is compartmented for security reasons. FHE enables cross-matching sources without breaking any compartment — authorized analysts access only the combined result, never the individual source. This is especially useful in international intelligence collaboration, where sharing primary sources is forbidden.

Defense and military operations

The Armed Forces operate operational-intelligence, logistics, personnel and mission data. Migration to PQC is an explicit priority of any serious military doctrine — sophisticated adversaries are conducting HNDL against Brazilian military communications today. FHE offers a dual path: collaborative capability (between services, between allies) and structured migration to PQC.

Sovereign AI over public data

The Brazilian State is increasingly using foreign LLMs and vision models to process documents, classify requests, generate responses to citizens. Each use is a surrender of algorithmic sovereignty. Under FHE, the State can use foreign models without handing over data — or, better yet, train its own models on citizen data without exposing the data.

Unified Social Registry and social-program targeting

Bolsa Família, BPC, state programs. Effective targeting requires cross-matching the Unified Social Registry, Brazilian Social Security (INSS), Revenue, SUS and state bases. Today that matching is partial

and delayed. Under FHE, continuous matching is possible without violating privacy. Result: **better targeting, less fraud, less undue exclusion**.

Public health and epidemiological surveillance

SUS has epidemiological data in volume and granularity that few countries have. Combined with pharmacy, lab and hospital data, it would enable early outbreak detection, real-world treatment effectiveness studies, pharmacovigilance. Under FHE, these combinations are possible without compromising individual privacy.

Federal Revenue Service and evasion detection

Cross-matching tax returns with bank flows, card activity, imports and real-estate operations is the heart of tax enforcement. Today it requires specific authorized operations. Under FHE, it can operate continuously, under verifiable mathematical auditing.

Diplomacy and confidential communications

Brazilian diplomatic communications today use classical cryptography vulnerable to CRQC. Migration to PQC is a priority. FHE adds an extra layer: it enables collaborative computation with allies without exposing primary sources.

CHAPTER V

PT EN

The Economics of the *State That Computes Without Seeing*.

Initial capex

COMPONENT	INVESTMENT
Founding team (senior cryptographers, ML, legal, project managers)	USD 6M – 10M / year
Licenses and tooling	USD 400k – 1.5M
Sovereign compute infrastructure	USD 5M – 15M
Strategic consulting	USD 1.5M – 4M
Regulatory and constitutional study	USD 800k – 2M
Integration with legacy systems across multiple agencies	USD 5M – 15M
Total year 1	**USD 19M – 47M**

Annual opex

PT EN

ITEM	ESTIMATE
Compute	USD 4M – 12M
Maintenance team	USD 6M – 12M
Audit	USD 1M – 3M
Annual opex	**USD 11M – 27M**

For the Brazilian federal government, with annual IT budgets in the order of USD 10–15 billion, this represents **less than 0.3%**. For a specific large agency, it is absorbable.

The return — six vectors

1. Detection of social-security and tax fraud

Estimated fraud at Brazilian Social Security (INSS): USD 5–15B annually. At Federal Revenue: USD 100–300B annually (tax gap). Capture via FHE-based cross-matching: **USD 5–50B annually in recovery**.

2. Social-program targeting

Bolsa Família, BPC and others have inclusion-error rates estimated at 5–10%. Reduction: **USD 2–8B annually**.

3. Digital sovereignty — protection against the CLOUD Act

Hard to quantify, but strategic. Protection against foreign access to Brazilian citizen data is worth political and moral capital.

4. PQC migration without rework

Estimated cost of emergency post-CRQC migration: **USD 1–5B**. Orderly migration starting fraction of that.

5. Publicly verifiable elections

Reduces the political cost of any challenge. Hard to quantify but decisive for democratic legitimacy.

6. Advantage in diplomacy and global governance

A Brazil leading in digital sovereignty gains voice in international forums. Priceless.

Business case

~USD 30M YEAR 1 INVESTMENT	~USD 18M STABILIZED ANNUAL OPEX
USD 10B+ VALUE ENABLED OVER 5 YEARS	100×+ EXPECTED ROI

PT EN

“For the Brazilian State, FHE is not an I[illegible] project. It is critical infrastructure of national sovereignty. ”

Geopolitical Competitive *Advantage*.

The geopolitics of the 21st century will be decided on three fronts: energy, data and compute capability. The State that masters all three will have real sovereignty. The one that loses any of them will have partial sovereignty. Brazil is well-positioned in energy. In data, partially well (volume) and partially poorly (technical capability). In compute capability, it depends critically on foreign vendors.

The three possible postures

1 — The Sovereign Republic

Focus on technological independence from foreign vendors. FHE as infrastructure to use foreign cloud without surrendering sovereignty. Explicit national PQC migration plan. Works as State policy.

2 — The Latin American Leader

Focus on building a regional (LATAM) consortium for privacy-preserving compute for intergovernmental collaboration. Brazil as articulator. Works for foreign policy.

3 — The Digital State Model

Focus on becoming a global reference for a digital State with verifiable privacy. Present the architecture in international forums (UN, OAS, Mercosur). Works to build soft power.

The cost of not taking a position

The scenario to make explicit: what happens if Brazil does not adopt FHE structurally in the next 36 months? Answer: **it remains dependent on foreign vendors for critical infrastructure**, loses voice in

international initiatives on data governance, arrives unprepared at CRQC in 2029, and discovers too late that it has handed algorithmic sovereignty to Big Tech.

CHAPTER VII

PT EN

24-Month *Roadmap*.

01

MONTHS 1–6 · LEARN

Institutional foundation

Set up an inter-ministerial working group. Hire talent (in partnership with public universities: USP, Unicamp, UFRJ, IMPA). Identify three candidate use cases. Align with the Brazilian Data Protection Authority (ANPD), the Attorney General's Office and the Institutional Security Office.

02

MONTHS 7–14 · BUILD

Inter-agency pilot

Build one end-to-end case. Recommendation: cross-matching Federal Revenue Service with Brazilian Social Security (INSS) under FHE to detect benefit fraud. Validate latency, key governance, traceability.

03

MONTHS 15–20 · FIRST REAL OPERATION

Real operation with legal basis

Launch the first real cross-match in production, with specific legal basis and backing from the Attorney General's Office. Begin formal dialogue with the Supreme Court about the architecture.

04

MONTHS 21–24 · NATIONAL CAPABILITY

PT EN

Adoption as critical infrastructure

Multiple cases. Formal national plan. Presentation in international forums. Possible public announcement of a digital sovereignty plan.

CHAPTER VIII

PT EN

Risks, Mitigations and *Pitfalls*.

1 · Institutional resistance across agencies

High probability. Each agency defends its silo. **Mitigation:** sponsorship at the highest level (Chief of Staff, Presidency). Without that, the project dies.

2 · Inability to hire talent

Public-sector salaries are incompatible with the market. **Mitigation:** partnerships with public universities. Temporary secondment of researchers. Center-of-excellence model.

3 · Resistance from foreign vendors

AWS, Azure, GCP will not facilitate the transition. **Mitigation:** negotiate as a premium customer. FHE does not require leaving the cloud — it requires using it differently.

4 · Legal misunderstanding

The Supreme Court, Attorney General's Office and prosecutors may misread the architecture. **Mitigation:** formal education. Present academic opinions.

5 · Computational cost at national volume

Mitigation: hybrid architecture. FHE only where it makes a difference.

Pitfall 1 · Treating it as an IT project

FHE must report to the highest level (Chief of Staff, Presidency), not to a ministry CIO.

Pitfall 2 · Underestimating the geopolitical dimension

This is not an IT decision. It is a sovereignty decision.

Pitfall 3 · Forgetting PQC migration

FHE and PQC must be treated as the same national program.

PT EN

A letter for the next decade of the *Brazilian State*.

The republic you serve was built on an old promise: that there exists a space, amid the world's inequality, where the State can be an instrument of protection, justice and collective development. That the citizen who entrusts the State with their most intimate data — their health, their income, their vote, their identity — is making a reasonable pact: I obey, you protect; I contribute, you do not betray.

This promise has lasted for decades. It survived dictatorships, redemocratizations, economic crises, technological transformations. It survived because it was — and largely still is — true. The citizens who pay taxes, contribute to social security, use SUS, vote in elections, register their children, do so, at heart, out of institutional trust in the republican promise.

But in the last fifteen years, without anyone having decreed it, the environment in which the State operates has changed entirely. Citizen data stopped being paper files kept in a public cabinet. It became petabytes processed in data centers, often at foreign vendors, under cryptography that will be obsolete in a few years, mediated by AI increasingly outsourced to companies headquartered in other nations. Each isolated technical decision was reasonable. The aggregate result is a situation no public leader would consciously design: Brazilian digital sovereignty has been partially surrendered, and almost no one noticed.

It is possible to turn back. FHE — Fully Homomorphic Encryption — allows the State to do everything it must do (cross-reference bases to detect fraud, train AI to improve services, use foreign cloud to scale) **without surrendering sovereignty**. It is possible, with the technology that exists today in 2026, to recover a significant part of control over citizen data without losing operational efficiency.

What is at stake is not a technical feature. It is the continuity of the republican promise in a fundamentally new technological world. It is the possibility for the Brazilian State to become again, unambiguously, an instrument of citizen protection — now with verifiable mathematical proof, not merely an institutional promise.

PT EN

> *“Within three years, some States will be ready for the 21st-century digital era. The question is whether Brazil will be one of them, or the one others will point to as an example of what to avoid.”*

There is a window. It is short. It is real. The rest is political courage.

APPENDIX A

PT EN

Executive *Glossary*.

FHE

Computation over encrypted data.

RLWE

Mathematical foundation of modern FHE and of NIST PQC.

CRQC

Cryptographically Relevant Quantum Computer. Estimate: 2029.

HNDL

Harvest Now, Decrypt Later — adversaries collect ciphertext today.

ML-KEM, ML-DSA

NIST post-quantum algorithms (FIPS 203, 204).

CLOUD ACT

2018 U.S. law allowing the U.S. government to compel data from American companies, even stored abroad.

EHDS

European Health Data Space — European model for secondary use of clinical data.

EUDI WALLET

European digital identity wallet.

PSI

Private Set Intersection. Central building block for cross-agency matching.

THRESHOLD CRYPTOGRAPHY

Distribution of a key across multiple parties with a required quorum.

PT EN

LATTIGO, OPENFHE, CONCRETE

FHE libraries.

APPENDIX B

PT EN

Vendors and *Partners*.

VENDOR	FOCUS
Tune Insight (Switzerland/EPFL)	Lattigo, focus on multi-institution collaborative research
Inpher (Switzerland/USA)	FHE+MPC, cases in finance and government
Duality (USA/Israel)	OpenFHE, partnership with NIH
Zama (Paris)	Concrete, TFHE
Stickybit (Brazil)	Brazilian technical boutique in FHE/PQC — the only Brazilian on this list

Brazilian academic centers

- **USP / IME-USP** — cryptography and security research
- **Unicamp / IC** — advanced cryptography
- **UFRJ / COPPE** — security and distributed systems
- **IMPA** — lattice mathematics

APPENDIX C

PT EN

30 Questions for the *Public Leader*.

Strategy

1. Do we have a national digital sovereignty plan?
2. Do we have a post-quantum migration plan?
3. How much of our digital operation depends on foreign cloud?
4. How much citizen data is hosted at a provider subject to the CLOUD Act?
5. Who is accountable for this in the org chart?

Priority use cases

6. How much do we lose per year to social-security fraud?
7. What is the avoidable tax gap?
8. What is the inclusion error in social programs?
9. Which cross-agency matches are paralyzed today?
10. Which scientific research depends on public data that is currently inaccessible?

Technical

11. Which FHE scheme for our first case?
12. Acceptable latency?
13. How do we integrate with each agency's legacy systems?
14. How do we manage keys across multiple agencies?
15. Is threshold cryptography compatible?

Cost

PT EN

16. FHE cost vs plaintext at national volume?
17. Build in-house (public university) or via consultancy?
18. Capex and opex over 24 months?
19. Political sponsor confirmed?

Regulation

20. Compliance with LGPD applied to the State?
21. Attorney General's Office opinion?
22. Dialogue with the Brazilian Data Protection Authority (ANPD)?
23. Does the Supreme Court understand the architecture?
24. Citizen communication?

Geopolitics

25. How much of our data can foreign states access via the CLOUD Act?
26. How do we protect diplomatic communications from HNDL?
27. How do we position ourselves in international forums on data governance?
28. How do we gain voice in post-quantum standards?
29. How do we protect national defense?
30. Worst-case scenario if other nations arrive first?

PT EN

~

Computable Sovereignty

Strategic eBook for senior public-sector leadership and digital sovereignty.

Volume I · Edition 2026 · Confidential distribution.

Set in Iowan Old Style and SF Pro.

— end —