PT EN

STRATEGIC EBOOK · EXECUTIVE LEVEL

FOR CEOS, CDOS, CTOS, CMOS AND BOARD MEMBERS OF THE LARGEST BRAZILIAN AND GLOBAL E-COMMERCE PLATFORMS AND MARKETPLACES

The Catalog That Does Not *Spy*.

How Fully Homomorphic Encryption enables marketplaces to deliver search, recommendation, fraud detection and personalization — without ever decrypting what belongs to the consumer.

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 modern large e-commerce platform is, simultaneously, the largest behavioral-data collection operation in consumer markets and the operation that most depends on that data to function. Every click, every search, every product viewed and abandoned, every purchase completed, every order returned, every review posted — all of it is raw material for the algorithms that decide what you see on your next visit. The entire marketplace operation depends on processing this data at scale and in real time.

Over the last five years, three things have converged to create a strategic problem that nobody in the industry is comfortable discussing:

1

REAL CONSENT FATIGUE

Conversion on funnels that require explicit consent has dropped 15–35% over the last 24 months. Users are exhausted.

2

TIGHTENING REGULATION

LGPD, GDPR and the AI Act are demanding proof of minimization. Fines in the hundreds of millions have already been imposed in the sector.

3

INFERENCE COST

Each billion AI calls per month costs millions. A proprietary model is the only path to economy at scale.

4

VENDOR DEPENDENCY

Those who outsource inference to OpenAI/Anthropic are handing data to parties who may become competitors.

FHE — Fully Homomorphic Encryption — unlocks an entirely new category of operation: **search, recommendation, fraud and personalization without decrypting the user**. It allows the to do everything it does today, with mathematical proof that the central server has never se consumer's individual history. And it enables anti-fraud consortia among competing marketplaces that are legally impossible today.

PT EN

> *"The next decade of digital retail will be defined by which marketplaces manage to deliver a personalized experience without persistent profiling — and by who does it first."*

THE DECISION

The question for the board is not "whether" to invest in defensible data architecture. It is how much it costs to wait until the regulator, the consumer, and the drop in conversion decide for you.

CHAPTER I

PT EN

The *Click* Industry.

E-commerce has become — without realizing it — one of the largest behavioral-data collection operations in the world. Every feature users love is, on the other side, a new layer of regulatory risk.

In 2010, a typical e-commerce operated on two types of data: registration and purchase history. That was it. Algorithmic decisions were simple — "those who bought X also bought Y". There was no serious public debate about privacy in digital retail, not there, not anywhere. Most consumers had no idea what a third-party cookie was.

In 2025, the same e-commerce processes hundreds of data points per session. Mouse movement, time on page, scroll depth, device, geolocation, time of day, IP, browser fingerprint, search history from other sites (via integrated pixels), typing patterns, payment preferences, post-purchase behavior. Each of these points becomes input for increasingly sophisticated algorithms. The algorithm decides which product appears first, which shipping fee to charge, which coupon to offer, when to send the abandoned-cart email.

What Changed in the Value Chain

PT EN

OPERATION	WHAT IT IS	RISK
Personalized search	Search results vary by user	Persistent profiling under LGPD
Recommendation	Suggestions based on longitudinal history	Special category when it includes health/orientation
Dynamic pricing	Prices varying by user	Algorithmic discrimination
Fraud detection	Model over behavioral patterns	Extensive data processing
Sales chat (live commerce)	Real-time conversation to close the sale	Intimate consumer content exposed

The Invisible Assets of a Marketplace

- **Longitudinal behavior** — years of each user, when they buy, what they return, when they come back
- **Catalog + queries** — a treasure trove for training proprietary embeddings
- **Fraud patterns** — millions of transactions labeled "ok/fraud" that no outside vendor has
- **Commercial intent** — the strongest signal that exists, more valuable than any social-media data
- **Sales chat** — conversations with sellers that reveal motivation and intimate context

What nobody told the consumer

A consumer who searches for "baby crib" does not understand, in any practical sense, that this search will enter a profile that lives for years on servers and will be cross-referenced with dozens of other searches to form a detailed picture of who they are. They believe they are running a search. They are also contributing to a persistent behavioral profile.

THE SILENT PROBLEM

PT EN

The current operation depends on consumers not understanding what they are handing over. Any journalistic or regulatory movement that increases that understanding undermines the operating foundation. These movements are happening simultaneously on three continents.

> *"The question for the marketplace board is not whether the current architecture is sustainable. It is how long until the first public decision reshapes the sector."*

CHAPTER II

PT EN

The Regulatory *Siege*.

Three continents, three converging regulations, and a consumer fatigue that no one has yet priced in.

LGPD and the Brazilian interpretation

LGPD does not classify behavioral data as a special category — but it requires a robust legal basis for processing, and the Brazilian Data Protection Authority (ANPD) has been interpreting "legitimate interest" increasingly narrowly. In 2025 the authority opened an investigation against a large marketplace for using search data for cross-sell without adequate consent. It will be the first of many.

GDPR and the cookie nightmare

GDPR turned the cookie consent banner into a permanent operating cost. More importantly: national Data Protection Authorities regularly fine sites that collect more than they need. The TCF (Transparency and Consent Framework) that underpins European behavioral advertising has already been partially invalidated by the Belgian authority. The industry operates in an expanding gray zone.

European AI Act

The AI Act, phased in through 2027, classifies AI systems that assess consumers for credit, pricing or ranking as high-risk. Marketplaces that do dynamic pricing, fraud risk scoring, or seller ranking are in the crosshairs. Estimated compliance cost per system: **six to seven figures**.

BIPA and US class actions

The Illinois Biometric Information Privacy Act (BIPA) generated billion-dollar settlements against Facebook and Google for facial recognition use. Marketplaces with biometric features (AR try-on, image

search) are in the crosshairs of the next wave.

PT EN

Consent fatigue

This is the least discussed and most important part for marketplaces. Conversion on funnels requiring explicit consent has dropped 15–35% over the past 24 months on most measured platforms. **Users are tired.** Every extra "I accept" click the marketplace asks for is a lost conversion. The traditional solution — asking for more consent — no longer scales.

FHE offers a different path: an architecture where data is never "processed" in the legal sense, because it remains encrypted. This drastically reduces the need for robust consent, restoring conversion and simplifying UX.

The cost of inaction

RISK	PROBABILITY 5 YEARS	IMPACT
LGPD/GDPR fine for weak legal basis	High	2–4% of global revenue
BIPA class action over a biometric feature	Medium	USD 100M–650M
Feature blocked by the AI Act	High in the EU	Loss of regional market
Consent fatigue → drop in conversion	Certain	Silent loss, hard to measure
Reputational crisis after a breach	Medium	12–24 months of impact

CHAPTER III

PT EN

FHE in Executive *Language*.

No mathematics. What the board needs to understand.

A transparent vault. You see that something is inside, you do not see what it is. You manipulate the contents from outside — add, multiply, compare, run entire recommendation models — without ever opening it. You return it sealed. This is FHE.

The conceptual leap

All cryptography your marketplace uses today protects data in transit (TLS) and at rest (AES). The third state — in use, during processing — has always required plaintext. That is the instant when the search engine accesses the user's history in plaintext. It is where the recommendation algorithm runs. It is where the fraud system analyzes patterns. **FHE eliminates the third state.**

How it works

> ANALOGY FOR THE MARKETPLACE
>
> The user profile remains permanently encrypted on the server with the user's own key (or with the platform's key under a threshold scheme). The recommendation engine runs over the encrypted profile. It returns an encrypted suggestion. The user's front-end decrypts locally. At no point has the central server seen the individual history in plaintext.

FHE vs alternatives

PT EN

TECHNOLOGY	PROMISES	FAILS
De-identification	"We removed identifiers"	Trivial re-identification via linkage
TEE	"The chip isolates"	Trusts the manufacturer; vendor lock-in
Federated Learning	"Data stays on the phone"	Gradients leak data
Differential Privacy	"We added noise"	Poor for individual personalization
FHE	**"Server never sees in plaintext"**	**High computational cost — but decreasing**

The cost myth

FHE is expensive for billion-call volumes — that is the honest argument against it. The answer is a hybrid architecture: use FHE in the sensitive core (persistent profile, deep personalized recommendation, collaborative fraud) and keep the rest of the operation on traditional architecture. For a Brazilian top-10 marketplace, the total investment is below 0.2% of the IT budget — comparable to the cost of a single payment platform migration.

CHAPTER IV

PT EN

Use Cases by *Line of Business*.

Private semantic search

Search is the #1 direct-ROI use case in any marketplace. Every percentage point of improvement in search conversion is worth millions. Today the improvement depends on personalizing results per user — which requires a persistent plaintext profile.

Under FHE: the user profile remains encrypted, the search engine computes rankings over the encrypted profile, and returns personalized results without the server seeing the history. **Conversion improves without persistent profiling.**

Contextual recommendation without profiling

"Why are you seeing this" — personalized recommendation is the core asset of any marketplace. Today it requires plaintext history. Under FHE, the algorithm runs over encrypted history, and the recommendation appears to the user without the central server ever seeing what they bought.

Collaborative fraud detection between marketplaces

This is the case where FHE unlocks something unique. Fraud — chargebacks, mule accounts, fake sellers, review purchasing, ranking manipulation — is a sector-wide problem. Each marketplace fights it in isolation, with limited effectiveness because fraudsters move between platforms. Effective fighting requires cooperation between competing marketplaces. Today impossible.

Under FHE with PSI (Private Set Intersection): marketplaces encrypt lists of tax IDs, IPs and suspicious patterns, discover **only the intersection** — those who appear in three or more platforms with fraud patterns. Without revealing entire databases. **It is a sector-wide defense that literally does not exist today.**

Product description generation under a proprietary fine-tune

A top marketplace has 100M+ SKUs. The catalog needs descriptions, titles, bullets, alt-text, SEO, in multiple languages. Today this requires sending SKUs to an external LLM (expensive, commoditized, data-leaking). Under FHE on a proprietary model: descriptions are generated over encrypted data; the LLM operator (even if it is a vendor) never sees the proprietary catalog.

Customer service without exposing history

80% of customer service contacts are repetitive: "where is my order", "how do I return", "my boleto expired". The human agent needs to see the history. Under FHE, the chatbot operates on encrypted history, returning answers without persisting the interaction. The human agent sees only what is needed during the call and archives nothing afterwards.

Vendor intelligence and seller experience

Marketplaces use sales data to help sellers sell better — price suggestions, listing improvements, demand prediction. That data is the marketplace's IP that sellers cannot see in detail. Under FHE, suggestions can be delivered to the seller without the seller ever accessing the models or other sellers' data.

AR try-on without storing the image

Virtual makeup, virtual clothing, virtual glasses. Every try-on involves 3D facial mapping processed on a server. Under FHE, the mapping happens locally on the phone and virtual pigments are applied under encryption. The marketplace receives aggregated metrics ("X users tried lipstick Y") without storing the image.

Defensible dynamic pricing

Dynamic pricing is legally sensitive because it can become algorithmic discrimination. Under FHE, the pricing algorithm runs over encrypted user data, returning a price without the central system having seen the justifying data. This offers a robust defense against discrimination claims.

Live commerce and sales chat

PT EN

Real-time conversation between seller and buyer is the fastest-growing channel. Each conversation contains intimate information: motivation, context, preferences. Today, it sits on the marketplace server. Under FHE, the conversation can happen with end-to-end encryption, and the marketplace receives only aggregated metrics (close rate, average time).

CHAPTER V

PT EN

The Economics of the *Marketplace That Does Not See*.

Initial capex

COMPONENT	INVESTMENT
Founding team (crypto + ML eng + PM + legal)	USD 4M – 7M / year
Licenses and tooling	USD 300k – 1M
Compute infrastructure	USD 1.5M – 4M
Strategic consulting	USD 800k – 2M
Regulatory study	USD 300k – 800k
Integration with core platform	USD 1.5M – 4M
Total year 1	**USD 8M – 17M**

Annual opex

PT EN

ITEM	ESTIMATE
Compute	USD 2M – 6M
Maintenance team	USD 4M – 7M
Audit	USD 400k – 1M
Stabilized annual opex	**USD 6.4M – 14M**

For a Brazilian top-10 marketplace with revenue above USD 5B, this represents between **0.15% and 0.3% of revenue**.

The return — five vectors

1. Conversion recovery from consent fatigue

Conversion dropped 15–35% in funnels with robust consent flows. For a USD 5B marketplace with a current conversion rate of 2–4%, recovering one percentage point is worth **USD 50–150M per year**.

2. Collaborative fraud mitigation

Estimated sector fraud: 1–3% of revenue. For a USD 5B marketplace that is USD 50–150M of annual exposure. Capture via PSI: **USD 15–50M per year**.

3. Reduced inference cost

Inference outsourced to OpenAI/Anthropic at billion-call scale costs millions per month. A proprietary model under FHE captures that saving: **USD 30–100M per year over three years**.

4. Reduced regulatory risk

Expected exposure to fines: USD 50–200M NPV. Hedge: **USD 20–80M of insurance value**

PT EN

5. Brand differentiation for Gen Z

"The marketplace that respects your data" as a premium narrative. Hard to quantify but measurable in retention and LTV.

Business case

~USD 12M YEAR 1 INVESTMENT	~USD 10M STABILIZED ANNUAL OPEX
USD 200M+ VALUE ENABLED IN 5 YEARS	15×–30× EXPECTED ROI IN 5 YEARS

> *"For any top-10 marketplace, FHE is the digital transformation investment with the highest return asymmetry available in 2026."*

CHAPTER VI

PT EN

Competitive Advantage and *Positioning*.

Marketplaces are the industry that loses the most when trust collapses, and the first to feel it when consumers get tired. Every new feature that asks for consent adds a bit of friction. At some point, the friction becomes systemic drag — and competitors that offer the same value with less drag win.

The three positionings

1 — The Marketplace That Does Not Spy on You

Focus on direct communication with Gen Z. Public privacy manifesto. Works best for premium marketplaces or D2C brand-first.

2 — The Sector Anti-Fraud Orchestrator

Focus on building an FHE consortium among marketplaces. Captures the sector-organizer role. Works for the top 3.

3 — The Sovereign Marketplace

Focus on a proprietary AI model without dependence on OpenAI/Anthropic. Inference sovereignty as a differentiator. Works for large marketplaces that want to become technical platforms.

The cost of not positioning

The scenario to spell out: what happens if none of the large Brazilian marketplaces structurally adopts FHE? Answer: **they will remain dependent on OpenAI/Anthropic/Google**, paying growing margins,

delivering data to parties that may become direct competitors. In five years, the gap will be structural and expensive to reverse.

CHAPTER VII

PT EN

The *24-Month* Roadmap.

01

MONTHS 1–6 · LEARN

Foundation and capability

Hire a founding crypto engineer. Identify three use cases. Align with legal and the DPO.

02

MONTHS 7–14 · BUILD

Internal pilot

Build one end-to-end case. Recommendation: fraud detection under FHE OR encrypted personalized recommendation for a segment.

03

MONTHS 15–20 · LAUNCH BETA

Closed program

Launch to a user segment. Measure conversion, NPS, latency. Compare against a control group.

04

MONTHS 21–24 · ANNOUNCE

Launch and narrative

Campaign. Manifesto. Possibly the first anti-fraud consortium with other marketplaces.

CHAPTER VIII

PT EN

Risks, Mitigations and *Pitfalls*.

1 · Computational cost at billion-call volume

High probability. **Mitigation:** hybrid architecture. FHE only in the sensitive core. The rest stays on traditional architecture.

2 · Inability to hire talent

Mitigation: partnership with specialized consulting.

3 · Internal resistance from the growth team

The growth team depends on aggressive personalization. It will resist. **Mitigation:** show that FHE preserves personalization.

4 · Competitor announces first

Mitigation: speed.

Pitfall 1 · Treating it as an IT project

FHE must report to the CDO/CMO, not the CIO.

Pitfall 2 · Communicating too early

Announcing before a working product generates backlash.

Pitfall 3 · Forgetting key governance

Who custodies the user's key? UX is half of the project.

PT EN

A letter to the next decade of *digital retail*.

The industry you lead grew on an old promise: that retail can be cheaper, more convenient, more personalized when intermediated by software. That the consumer who prefers to buy online instead of in the physical store gains time, price and variety. That the marketplace is the infrastructure that makes this convenience possible.

That promise has lasted two decades. It survived bubbles, crises, new technologies. It endured because it was — and largely still is — true. Consumers who buy online instead of in the physical store do so for real, practical reasons.

But over the last fifteen years, without anyone decreeing it, the relationship between marketplace and consumer has changed in nature. The consumer is no longer someone who enters the site, searches for the product, buys, and leaves. They have become a continuous source of behavioral data feeding ever more sophisticated algorithms. The aggregate result is an operation that extracts value from consumers in ways they would never consciously consent to.

It is possible to walk this back without losing the benefits. FHE allows you to continue offering personalization, recommendation and fraud detection — **without ever seeing the individual consumer**.

> *"In three years, some marketplace will lead. The question is whether it will be yours, or the one you will have to look at as a reference."*

There is a window. It is narrow. It is real. The rest is courage.

APPENDIX A

PT EN

Executive *Glossary*.

FHE

Computation over encrypted data.

PSI

Private Set Intersection — discovering the intersection of datasets without revealing the rest.

CKKS, BFV/BGV, TFHE

FHE schemes.

EMBEDDINGS

Vector representations of products and queries that underpin semantic search.

LGPD, GDPR, AI ACT, BIPA

Relevant regulations.

LATTIGO, OPENFHE, CONCRETE

FHE libraries.

APPENDIX B

PT EN

Vendors and *Partners*.

VENDOR	FOCUS
Zama	Concrete, TFHE, focus on developer experience
Duality	OpenFHE, focus on finance and analytics
Inpher	FHE+MPC for finance
Tune Insight	Lattigo
Stickybit	Brazilian technical boutique

APPENDIX C

PT EN

30 Questions for the *CDO/CMO/CTO*.

Strategy

1. Who understands advanced cryptography in our company?
2. What is our exposure to behavioral data processing?
3. How many AI vendors have access to user data?
4. Inventory of which data leaves the marketplace?
5. Conversion rate vs consent rate — do we have data?

Priority use cases

6. How much is one recovered conversion point worth?
7. How much do we lose to fraud we cannot fight alone?
8. How much do we spend on outsourced inference per month?
9. Which new features were not launched due to privacy concerns?
10. Would other platforms join an anti-fraud consortium?

Technical

11. Which FHE scheme for our first use case?
12. Acceptable latency?
13. How do we integrate with the core platform?
14. How do we manage user keys?
15. Is the key UX viable?

Cost

PT EN

16. FHE cost vs plaintext?
17. Build in-house or via vendor?
18. 24-month capex and opex?
19. C-level sponsor confirmed?

Regulation

20. Demonstrable LGPD/GDPR compliance?
21. Dialogue with the Brazilian Data Protection Authority (ANPD)?
22. Consumer communication?

Commercial

23. How do we price the advantage?
24. Which segments would pay for verifiable privacy?
25. Would current AI vendors accept FHE?
26. Is inference sovereignty worth the investment?
27. What is the brand narrative?
28. Internal case study?
29. Worst-case scenario if a competitor announces first?
30. Worst-case scenario if the Brazilian Data Protection Authority imposes heavy rules?

PT EN

The Catalog That Does Not Spy

Strategic eBook for senior management at e-commerce platforms and marketplaces.
Volume I · Edition 2026 · Confidential distribution.

Set in Iowan Old Style and SF Pro.

— end —