EBOOK ESTRATÉGICO · ALTA GESTÃO

PARA CEOS, CDOS, CTOS, CMOS E CONSELHOS DOS MAIORES E-COMMERCES E MARKETPLACES BRASILEIROS E GLOBAIS

O Catálogo que Não *Espia*.

Como a Criptografia Totalmente Homomórfica permite ao marketplace entregar busca, recomendação, fraude e personalização — sem nunca decifrar o que pertence ao consumidor.

VOLUME I · EDIÇÃO 2026 · CONFIDENCIAL

SUMÁRIO

O que você vai *ler*.

- Apêndices

00 · SUMÁRIO EXECUTIVO

O argumento em *uma* página.

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

O grande e-commerce moderno é, simultaneamente, a maior operação de coleta de dado comportamental do consumo e a operação que mais depende desse dado para funcionar. Cada clique, cada busca, cada produto visualizado e abandonado, cada compra efetuada, cada pedido devolvido, cada review publicado — tudo isto é matéria-prima para os algoritmos que decidem o que você vê na próxima visita. A operação inteira do marketplace depende de processar esse dado em escala e em tempo real.

Nos últimos cinco anos, três coisas convergiram para criar um problema estratégico que ninguém na indústria está confortável em discutir:

1

CONSENT FATIGUE REAL

Conversão de funis com consentimento explícito caiu 15-35% nos últimos 24 meses. O usuário cansou.

2

REGULAÇÃO APERTANDO

LGPD, GDPR e AI Act exigindo prova de minimização. Multas em centenas de milhões já aplicadas no setor.

3

CUSTO DE INFERÊNCIA

Cada bilhão de chamadas de IA por mês custa milhões. Modelo próprio é única forma de economia em escala.

4

DEPENDÊNCIA DE FORNECEDOR

Quem terceiriza inferência a OpenAI/Anthropic está entregando dado a quem pode virar concorrente.

FHE — Criptografia Totalmente Homomórfica — destrava uma categoria inteira nova de operação: **busca, recomendação, fraude e personalização sem decifrar o usuário**. Permite ao marketplace fazer tudo o que faz hoje, com prova matemática de que o servidor central nunca viu o histórico individual do consumidor. E permite consórcios anti-fraude entre marketplaces concorrentes que hoje são juridicamente impossíveis.

> *"A próxima década do varejo digital será definida por quais marketplaces conseguirem entregar experiência personalizada sem profiling persistente — e por quem souber fazê-lo primeiro."*

A DECISÃO

A pergunta para o conselho não é "se" investir em arquitetura de dado defensável. É quanto custa esperar até que o regulador, o consumidor, e a queda de conversão decidam por você.

CAPÍTULO I

A Indústria do *Clique*.

O e-commerce virou — sem perceber — uma das maiores operações de coleta de dado comportamental do mundo. Cada feature que o usuário ama é, do outro lado, uma camada nova de risco regulatório.

Em 2010, um e-commerce típico operava sobre dois tipos de dado: cadastro e histórico de compra. Era isso. As decisões algorítmicas eram simples — "quem comprou X também comprou Y". Não havia, nem ali nem em lugar nenhum, debate público sério sobre privacidade no varejo digital. A maior parte dos consumidores não fazia ideia do que era cookie de terceiro.

Em 2025, o mesmo e-commerce processa centenas de pontos de dado por sessão. Movimento de mouse, tempo de permanência em página, scroll depth, dispositivo, geolocalização, hora do dia, IP, browser fingerprint, histórico de busca de outros sites (via pixels integrados), padrão de digitação, preferência de pagamento, comportamento pós-compra. Cada um desses pontos vira input para algoritmos cada vez mais sofisticados. O algoritmo decide qual produto aparece primeiro, qual frete cobrar, qual cupom oferecer, em qual momento enviar o e-mail de carrinho abandonado.

O que mudou na cadeia de valor

OPERAÇÃO	O QUE É	RISCO
Busca personalizada	Resultado de busca varia por usuário	Profiling persistente sob LGPD
Recomendação	Sugestão baseada em histórico longitudinal	Categoria especial quando inclui saúde/orientação
Pricing dinâmico	Preço variando por usuário	Discriminação algorítmica
Detecção de fraude	Modelo sobre padrão de comportamento	Tratamento extensivo de dado
Chat de venda (live commerce)	Conversa em tempo real para fechar venda	Conteúdo íntimo do consumidor exposto

Os ativos invisíveis do marketplace

- **Comportamento longitudinal** — anos de cada usuário, quando ele compra, o que devolve, quando volta
- **Catálogo + queries** — um treasure trove para treinar embeddings próprios
- **Padrão de fraude** — milhões de transações com label "ok/fraude" que nenhum vendor de fora tem
- **Intent comercial** — sinal mais forte que existe, mais valioso que qualquer dado de redes sociais
- **Chat de venda** — conversas com vendedor que revelam motivação e contexto íntimo

O que ninguém disse ao consumidor

O consumidor que faz uma busca por "berço para bebê" não compreende, em qualquer sentido prático, que aquela busca vai entrar em um perfil que vive anos em servidores e que será cruzado com dezenas de outras buscas para formar uma imagem detalhada de quem ele é. Ele acredita estar fazendo uma busca. Está, também, contribuindo para um perfil comportamental persistente.

O PROBLEMA SILENCIOSO

A operação atual depende do consumidor não compreender o que está entregando. Qualquer movimento jornalístico ou regulatório que aumente essa compreensão derruba a base de funcionamento. Esses movimentos estão acontecendo simultaneamente em três continentes.

> *“A pergunta para o conselho do marketplace não é se a arquitetura atual é sustentável. É quanto tempo falta até a primeira decisão pública mudar o setor.”*

CAPÍTULO II

O Cerco *Regulatório*.

Três continentes, três regulações convergentes, e uma fadiga do consumidor que ninguém ainda precificou.

LGPD e a interpretação brasileira

A LGPD não classifica dado comportamental como categoria especial — mas exige base legal robusta para tratamento, e a ANPD vem interpretando "legítimo interesse" de forma cada vez mais restritiva. Em 2025 a autoridade abriu investigação contra um grande marketplace por uso de dado de busca para cross-sell sem consentimento adequado. Será o primeiro de muitos.

GDPR e o pesadelo dos cookies

GDPR transformou o cookie consent banner em um custo operacional permanente. Mais importante: as CNILs nacionais estão multando regularmente sites que coletam mais do que precisariam. O TCF (Transparency and Consent Framework) que sustenta a publicidade comportamental europeia já foi parcialmente invalidado pela autoridade belga. A indústria opera em zona cinza crescente.

AI Act europeu

O AI Act, em vigor escalonado até 2027, classifica sistemas de IA que avaliam consumidor para crédito, preço, ou ranking como alto risco. Marketplaces que fazem pricing dinâmico, scoring de risco de fraude, ou ranking de vendedor estão na mira. Custo de compliance estimado por sistema: **6 a 7 dígitos**.

BIPA e classes nos EUA

O Illinois Biometric Information Privacy Act (BIPA) gerou acordos de bilhões contra Facebook e Google por uso de reconhecimento facial. Marketplaces com features biométricas (try-on AR, busca por

imagem) estão na mira da próxima onda.

A fadiga do consentimento

Esta é a parte menos discutida e a mais importante para marketplace. Conversão de funis que exigem consentimento explícito caiu 15-35% nos últimos 24 meses na maioria das plataformas medidas. **O usuário cansou**. Cada clique extra de "aceito" que o marketplace pede é conversão perdida. A solução tradicional — pedir mais consentimento — não escala mais.

FHE oferece um caminho diferente: arquitetura onde o dado nunca é "tratado" no sentido legal, porque permanece cifrado. Isso reduz drasticamente a necessidade de consentimento robusto, devolvendo conversão e simplificando UX.

O custo de não agir

RISCO	PROBABILIDADE 5 ANOS	IMPACTO
Multa LGPD/GDPR por base legal frágil	Alta	2-4% do faturamento global
Class action BIPA por feature biométrica	Média	USD 100M-650M
Bloqueio de feature por AI Act	Alta na UE	Perda de mercado regional
Consent fatigue → queda de conversão	Certa	Perda silenciosa, difícil de medir
Crise reputacional pós-breach	Média	12-24 meses de impacto

CAPÍTULO III

FHE em Linguagem *Executiva*.

Sem matemática. O que a diretoria precisa entender.

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

O salto conceitual

Toda criptografia que seu marketplace usa hoje protege dado em trânsito (TLS) e em repouso (AES). O terceiro estado — em uso, durante processamento — sempre exigiu plaintext. É nesse instante que o motor de busca acessa o histórico do usuário em claro. É onde o algoritmo de recomendação roda. É onde o sistema de fraude analisa padrão. **FHE elimina o terceiro estado.**

Como funciona

> ANALOGIA PARA O MARKETPLACE
>
> O perfil do usuário fica permanentemente cifrado no servidor com chave do próprio usuário (ou com chave da plataforma sob threshold). O motor de recomendação roda sobre o perfil cifrado. Devolve sugestão cifrada. O front-end do usuário decifra localmente. Em nenhum momento o servidor central viu o histórico individual em claro.

FHE vs alternativas

TECNOLOGIA	PROMETE	FALHA
Anonimização	"Removemos identificadores"	Re-identificação trivial via cruzamento
TEE	"O chip isola"	Confia no fabricante; vendor lock-in
Federated Learning	"Dado fica no celular"	Gradientes vazam dado
Differential Privacy	"Adicionamos ruído"	Ruim para personalização individual
FHE	**"Servidor nunca vê em claro"**	**Custo computacional alto — mas decrescente**

O mito do custo

FHE é caro para volume bilionário de chamadas — esse é o argumento honesto contra. A resposta é arquitetura híbrida: usar FHE no núcleo sensível (perfil persistente, recomendação personalizada profunda, fraude colaborativa) e manter o resto da operação em arquitetura tradicional. Para um marketplace top 10 brasileiro, o investimento total fica abaixo de 0,2% do orçamento de TI — comparável ao custo de uma única migração de plataforma de pagamento.

CAPÍTULO IV

Casos de Uso por *Linha*.

Busca semântica privada

Busca é o caso #1 de ROI direto em qualquer marketplace. Cada ponto percentual de melhoria em conversão de busca vale milhões. Hoje a melhoria depende de personalizar resultado por usuário — o que exige perfil persistente em claro.

Sob FHE: o perfil do usuário fica cifrado, o motor de busca computa rankings sobre o perfil cifrado, devolve resultado personalizado sem que o servidor veja o histórico. **Conversão melhora sem profiling persistente.**

Recomendação contextual sem profiling

"Por que você está vendo isto" — recomendação personalizada é o ativo central de qualquer marketplace. Hoje exige histórico em claro. Sob FHE, o algoritmo roda sobre o histórico cifrado, e a recomendação aparece para o usuário sem que o servidor central nunca veja o que ele comprou.

Detecção de fraude colaborativa entre marketplaces

Este é o caso onde FHE destrava algo único. Fraude — chargeback, conta laranja, vendedor falso, compra de review, manipulação de ranking — é problema setorial. Cada marketplace combate isoladamente, com eficácia limitada porque os fraudadores migram entre plataformas. Combate eficaz exige cooperação entre marketplaces concorrentes. Hoje impossível.

Sob FHE com PSI (Private Set Intersection): marketplaces cifram listas de CPFs, IPs, padrões suspeitos, descobrem **apenas a interseção** — quem aparece em três ou mais plataformas com padrão de fraude. Sem revelar bases inteiras. **É defesa setorial que hoje literalmente não existe.**

Geração de descrição de produto sob fine-tune próprio

Marketplace top tem 100M+ de SKUs. Catálogo precisa de descrição, título, bullet, alt-text, SEO, em múltiplos idiomas. Hoje exige enviar SKU para LLM externa (caro, comoditizado, entrega dado). Sob FHE em modelo próprio: descrição é gerada sobre dado cifrado, o operador da LLM (mesmo que seja vendor) nunca vê o catálogo proprietário.

Atendimento ao cliente sem expor histórico

80% dos contatos de atendimento são repetitivos: "onde está meu pedido", "como troco", "boleto venceu". O atendente humano precisa ver o histórico. Sob FHE, o chatbot opera sobre histórico cifrado, devolvendo resposta sem persistir a interação. O atendente humano vê o necessário no momento da chamada e nada arquiva depois.

Vendor intelligence e seller experience

Marketplace usa dados de venda para ajudar vendedor a vender melhor — sugestões de preço, melhoria de listing, predição de demanda. Esse dado é IP do marketplace que vendor não pode ver detalhadamente. Sob FHE, sugestões podem ser entregues ao vendedor sem que o vendedor jamais acesse os modelos ou dados de outros vendedores.

Try-on AR sem armazenar imagem

Maquiagem virtual, roupa virtual, óculos virtual. Cada experimentação envolve mapeamento facial 3D processado em servidor. Sob FHE, o mapeamento acontece localmente no celular e a aplicação dos pigmentos virtuais sob cifra. Marketplace recebe métricas agregadas ("X usuárias provaram batom Y") sem armazenar imagem.

Pricing dinâmico defensável

Pricing dinâmico é juridicamente sensível porque pode virar discriminação algorítmica. Sob FHE, o algoritmo de precificação roda sobre dados cifrados do usuário, devolvendo preço sem que o sistema central tenha visto os dados que justificam. Isso oferece argumento defensivo robusto contra alegação de discriminação.

Live commerce e chat de venda

Conversa em tempo real entre vendedor e comprador é o canal que mais cresce. Cada conversa contém informação íntima: motivação, contexto, preferências. Hoje, isso fica em servidor do marketplace. Sob FHE, a conversa pode acontecer com criptografia de ponta a ponta, e o marketplace recebe apenas métricas agregadas (taxa de fechamento, tempo médio).

CAPÍTULO V

A Economia do *Marketplace que Não Vê*.

Capex inicial

COMPONENTE	INVESTIMENTO
Time fundador (cripto + ML eng + PM + jurídico)	R$ 4M – 7M / ano
Licenças e tooling	R$ 300k – 1M
Infra computacional	R$ 1.5M – 4M
Consultoria estratégica	R$ 800k – 2M
Estudo regulatório	R$ 300k – 800k
Integração com plataforma core	R$ 1.5M – 4M
Total ano 1	**R$ 8M – 17M**

Opex anual

ITEM	ESTIMATIVA
Compute	R$ 2M – 6M
Time de manutenção	R$ 4M – 7M
Auditoria	R$ 400k – 1M
Opex anual estabilizado	**R$ 6.4M – 14M**

Para um marketplace top 10 brasileiro com receita acima de R$ 5B, isto representa entre **0,15% e 0,3% do faturamento**.

O retorno — cinco vetores

1. Recuperação de conversão por consent fatigue

Conversão caiu 15-35% em funis com consentimento robusto. Para marketplace de R$ 5B com taxa de conversão atual de 2-4%, recuperar 1 ponto percentual vale **R$ 50-150M anuais**.

2. Combate a fraude colaborativa

Fraude estimada do setor: 1-3% da receita. Para marketplace de R$ 5B isto é R$ 50-150M de exposição anual. Captura via PSI: **R$ 15-50M anuais**.

3. Redução de custo de inferência

Inferência terceirizada a OpenAI/Anthropic em escala bilionária custa milhões mensais. Modelo próprio sob FHE captura economia: **R$ 30-100M anuais em três anos**.

4. Redução de risco regulatório

Exposição esperada a multas: R$ 50-200M VPL. Hedge: **R$ 20-80M de valor segurador**.

5. Diferenciação de marca para Gen Z

"Marketplace que respeita seu dado" como narrativa premium. Difícil de quantificar mas mensurável em retenção e LTV.

Caso de negócio

~R$ 12M INVESTIMENTO ANO 1	~R$ 10M OPEX ANUAL ESTABILIZADO
R$ 200M+ VALOR HABILITADO EM 5 ANOS	15×–30× ROI ESPERADO EM 5 ANOS

> *"Para qualquer marketplace top 10, FHE é o investimento de transformação digital com maior assimetria de retorno disponível em 2026."*

CAPÍTULO VI

Vantagem Competitiva e *Posicionamento*.

Marketplace é a indústria que mais perde quando a confiança colapsa, e a primeira a sentir quando o consumidor cansa. Cada nova feature que pede consentimento adiciona um pouco de fricção. Em algum ponto, a fricção vira atrito sistêmico — e os concorrentes que oferecerem o mesmo valor com menos atrito ganham.

Os três posicionamentos

1 — O Marketplace Que Não Te Espia

Foco em comunicação direta com Gen Z. Manifesto público sobre privacidade. Funciona melhor para marketplace premium ou D2C brand-first.

2 — O Articulador Anti-Fraude Setorial

Foco em construir consórcio FHE entre marketplaces. Captura papel de organizador setorial. Funciona para top 3.

3 — O Marketplace Soberano

Foco em modelo de IA próprio sem dependência de OpenAI/Anthropic. Soberania de inferência como diferencial. Funciona para marketplaces grandes que querem virar plataforma técnica.

O custo de não posicionar

O cenário a explicitar: o que acontece se nenhum dos grandes marketplaces brasileiros adotar FHE estruturalmente? Resposta: **vão continuar dependentes de OpenAI/Anthropic/Google**, pagando

margem crescente, entregando dado a quem pode virar concorrente direto. Em cinco anos, a diferença vai ser estrutural e cara reverter.

CAPÍTULO VII

Roadmap de *24 Meses*.

01

MESES 1–6 · APRENDER

Fundação e capacidade

Contratar cripto-engenheiro fundador. Identificar três casos de uso. Alinhar com jurídico e DPO.

02

MESES 7–14 · CONSTRUIR

Piloto interno

Construir um caso ponta a ponta. Recomendação: detecção de fraude sob FHE OU recomendação personalizada cifrada para um segmento.

03

MESES 15–20 · LANÇAR BETA

Programa fechado

Lançar para um segmento de usuários. Medir conversão, NPS, latência. Comparar contra grupo de controle.

04

MESES 21–24 · ANUNCIAR

Lançamento e narrativa

Campanha. Manifesto. Possível primeiro consórcio anti-fraude com outros marketplaces.

CAPÍTULO VIII

Riscos, Mitigações e *Armadilhas*.

1 · Custo computacional para volume bilionário

Alta probabilidade. **Mitigação:** arquitetura híbrida. FHE só no núcleo sensível. Resto fica em arquitetura tradicional.

2 · Não conseguir contratar talento

Mitigação: parceria com consultoria especializada.

3 · Resistência interna do time de growth

Time de growth depende de personalização agressiva. Resistirá. **Mitigação:** mostrar que FHE preserva personalização.

4 · Concorrente anuncia primeiro

Mitigação: velocidade.

Armadilha 1 · Tratar como projeto de TI

FHE deve reportar a CDO/CMO, não CIO.

Armadilha 2 · Comunicar cedo demais

Anunciar antes de produto funcional gera backlash.

Armadilha 3 · Esquecer governança de chave

Quem custodia a chave do usuário? UX é metade do projeto.

CAPÍTULO IX · MANIFESTO

Uma carta para a próxima década do *varejo digital*.

A indústria que vocês lideram cresceu sobre uma promessa antiga: a de que o varejo pode ser mais barato, mais conveniente, mais personalizado quando intermediado por software. Que o consumidor que prefere comprar online em vez de na loja física ganha tempo, preço e variedade. Que o marketplace é a infraestrutura que viabiliza essa conveniência.

Essa promessa atravessou duas décadas. Sobreviveu a bolhas, crises, novas tecnologias. Sobreviveu porque era — e em grande parte ainda é — verdadeira. Os consumidores que compram online em vez de na loja física fazem isso por razões práticas reais.

Mas nos últimos quinze anos, sem que ninguém tenha decretado, a relação entre marketplace e consumidor mudou de natureza. O consumidor deixou de ser quem entra no site, busca o produto, compra, vai embora. Tornou-se uma fonte contínua de dado comportamental que nutre algoritmos cada vez mais sofisticados. O resultado agregado é uma operação que extrai valor do consumidor de formas que ele nunca consentiria conscientemente.

É possível voltar atrás sem perder os benefícios. FHE permite continuar oferecendo personalização, recomendação, fraude detection — **sem nunca ver o consumidor individual**.

> *"Em três anos, algum marketplace vai liderar. A pergunta é se será o seu, ou aquele para quem você terá que olhar como referência."*

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

APÊNDICE A

Glossário *Executivo*.

FHE

Computação sobre dado cifrado.

PSI

Private Set Intersection — descobrir interseção entre bases sem revelar o resto.

CKKS, BFV/BGV, TFHE

Esquemas FHE.

EMBEDDINGS

Representações vetoriais de produtos e queries que sustentam busca semântica.

LGPD, GDPR, AI ACT, BIPA

Regulações relevantes.

LATTIGO, OPENFHE, CONCRETE

Bibliotecas FHE.

APÊNDICE B

Fornecedores e *Parceiros*.

VENDOR	FOCO
Zama	Concrete, TFHE, foco em developer experience
Duality	OpenFHE, foco em finanças e analytics
Inpher	FHE+MPC para finanças
Tune Insight	Lattigo
Stickybit	Boutique técnica brasileira

APÊNDICE C

30 Perguntas para o *CDO/CMO/CTO*.

Estratégia

1. Quem entende criptografia avançada na nossa empresa?
2. Qual exposição a tratamento de dado comportamental?
3. Quantos vendors de IA têm acesso aos dados de usuário?
4. Inventário de quais dados saem do marketplace?
5. Conversion rate vs taxa de consentimento — temos dados?

Casos prioritários

6. Quanto vale 1 ponto de conversão recuperado?
7. Quanto perdemos com fraude que não combatemos sozinhos?
8. Quanto gastamos em inferência terceirizada por mês?
9. Quais features novas não foram lançadas por privacidade?
10. Outras plataformas topariam consórcio anti-fraude?

Técnica

11. Esquema FHE para nosso primeiro caso?
12. Latência aceitável?
13. Como integramos com plataforma core?
14. Como gerenciamos chaves do usuário?
15. UX de chave é viável?

Custo

16. Custo FHE vs plaintext?
17. Construir interno ou via vendor?
18. Capex e opex 24 meses?
19. Sponsor C-level confirmado?

Regulação

20. Conformidade LGPD/GDPR demonstrável?
21. Diálogo com ANPD?
22. Comunicação ao consumidor?

Comercial

23. Como precificamos a vantagem?
24. Que segmentos pagariam por privacidade verificável?
25. Vendors de IA atuais aceitariam FHE?
26. Soberania de inferência vale o investimento?
27. Qual narrativa de marca?
28. Estudo de caso interno?
29. Pior cenário se concorrente anuncia primeiro?
30. Pior cenário se ANPD impuser regras pesadas?

O Catálogo que Não Espia

eBook estratégico para a alta gestão de e-commerces e marketplaces.
Volume I · Edição 2026 · Distribuição confidencial.

Composto em Iowan Old Style e SF Pro.

— fim —