EBOOK ESTRATÉGICO · ALTA GESTÃO

PARA CEOS, CDOS, CMOS, DIRETORES DE INOVAÇÃO E CONSELHOS DAS MAIORES CASAS DE COSMÉTICOS DO MUNDO

O Espelho que *Não Vê*.

Como a Criptografia Totalmente Homomórfica redefine a relação entre marca, consumidora e dado biométrico — e por que a primeira casa a entender isto vai dominar a próxima década do beauty.

VOLUME I · EDIÇÃO 2026 · CONFIDENCIAL

SUMÁRIO

O que você vai *ler*.

Este eBook é um documento de decisão. Foi escrito para ser lido em uma reunião de comitê executivo, em uma viagem de avião, ou em um sábado de manhã antes de uma decisão de investimento.

00 Sumário Executivo 3
O argumento em uma página

I A Indústria do Espelho 5
Por que cosmético virou — sem perceber — uma indústria de dado biométrico

II O Cerco Regulatório 9
LGPD, GDPR, AI Act e o fim da era do consentimento performático

III FHE em Linguagem Executiva 13
O que é, sem matemática — e o que muda

IV Casos de Uso por Linha de Produto 17
Skincare, makeup, haircare, fragrância, wellness, derma e luxo

V A Economia do Espelho Cego 27
Custos reais, ROI, e onde o dinheiro aparece

VI Vantagem Competitiva e Posicionamento 33
Por que isto é narrativa de marca, não TI

VII Roadmap de 24 Meses 37
Da fase de aprendizado ao primeiro produto público

VIII Riscos, Mitigações e Armadilhas 43
O que pode dar errado e como evitar

IX Manifesto 47
Uma carta para a próxima década do beauty

· Apêndices 51
Glossário, fornecedores, 30 perguntas para o CTO

00 · SUMÁRIO EXECUTIVO

O argumento em *uma* página.

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

A indústria cosmética dos últimos cinco anos transformou-se silenciosamente em uma indústria de dado biométrico íntimo. Apps que pedem a selfie diária da consumidora. Diagnósticos de pele, cabelo e microbioma. Genoma para "skincare personalizado". Wearables que medem hidratação e melanina. Comportamento de compra que é proxy direto de autoestima, idade biológica e estado emocional.

Esta transformação aconteceu sem que o modelo de governança de dado, a arquitetura técnica e a narrativa pública de marca acompanhassem. O resultado é uma indústria que opera em zona cinza legal crescente, com risco reputacional acumulado, e dependente de uma promessa de privacidade que **não pode ser provada** — apenas declarada.

Ao mesmo tempo, três forças estão convergindo:

1

REGULAÇÃO APERTANDO

LGPD art. 11, GDPR cat. especial, AI Act europeu — todos exigindo prova de minimização, não promessa.

2

CONSUMIDOR CÉTICO

Gen Z compra valores. "Não vendemos seu dado" virou commodity; "não vemos seu dado" é o próximo nível.

3

FHE MADURO

Lattigo, OpenFHE, Concrete já viáveis em produção para inferência sobre imagem pequena, análise estatística, scoring.

4

JANELA ABERTA

Nenhum grande player de cosméticos cravou narrativa de "privacidade matemática". Quem chegar primeiro define a categoria.

A tese deste eBook é direta:

> *“A próxima década do beauty será definida pela primeira casa que disser, com prova matemática: nós nunca vemos o seu rosto.”*

FHE — *Fully Homomorphic Encryption*, ou Criptografia Totalmente Homomórfica — é a tecnologia que torna esta afirmação **verdadeira e auditável**. Não é uma promessa de gestão. É um teorema matemático.

O custo computacional ainda é alto, e isso será discutido com honestidade. Mas a curva de adoção, os casos onde já é viável, e o valor de marca que se cria ao ser *o primeiro* a fazê-lo justificam um investimento que, em qualquer cenário, devolve mais em narrativa do que custa em infraestrutura.

> **A DECISÃO**
>
> Não é "se" a indústria cosmética vai adotar computação privada. É "quem" vai liderar a mudança e capturar o prêmio narrativo. Este eBook é um mapa para essa decisão.

CAPÍTULO I

A Indústria do *Espelho*.

Como uma indústria centenária de pigmentos, óleos e fragrâncias se transformou — sem decreto, sem manifesto, sem perceber — em uma das maiores operações de coleta de dado biométrico íntimo do planeta.

Em 2010, uma cliente da Lancôme entrava em uma loja de departamento, conversava com uma consultora, experimentava três bases, comprava uma. A transação deixava como rastro: um nome em uma ficha, um número de cartão, talvez um e-mail para a newsletter. Era isso.

Em 2025, a mesma cliente abre um aplicativo, autoriza a câmera, posa para uma análise de pele, recebe um diagnóstico de oleosidade, poros, hidratação, pigmentação, idade aparente, "marca de cansaço". O app armazena a foto. Cruza com histórico de compra. Cruza com geolocalização (clima local, UV index, poluição). Cruza com ciclo menstrual se ela usa um app integrado. Cruza com dieta se ela conectou outro. Em alguns produtos, cruza com **sequência de DNA** coletada via swab bucal enviado pelo correio.

Tudo isso é feito sob a promessa genérica de "personalização". E tudo isso é tecnicamente — e cada vez mais juridicamente — **processamento de dado pessoal sensível em categoria especial**.

O que mudou na cadeia de valor

Cosmético sempre foi uma indústria de produto físico vendida com narrativa de identidade. O que mudou nos últimos anos não é o produto — é que a narrativa virou *operacional*. A "personalização" deixou de ser um discurso de marketing e virou uma promessa concreta que precisa ser cumprida com algoritmo, dado e infraestrutura.

Esta transição introduziu cinco novos ativos na operação de uma casa de cosméticos:

ATIVO	O QUE É	RISCO REGULATÓRIO
Imagem facial	Selfie, vídeo, mapeamento 3D para análise de pele, maquiagem virtual, "experimentação"	Biométrico — categoria especial
Imagem capilar	Foto de couro cabeludo, fio, cor natural, padrão de queda	Saúde — categoria especial
Genoma / variantes	SNPs relevantes para metabolismo cutâneo, pigmentação, sensibilidade	Saúde + identificação eterna
Microbioma	Composição bacteriana da pele, do couro cabeludo, axilar	Quase tão identificável quanto DNA
Comportamento íntimo	Compra de produtos para autoestima, sexualidade, ciclo, idade — proxies emocionais	Perfilamento sensível

Nenhum desses cinco ativos existia, em escala, na indústria cosmética em 2015. Em 2026 são parte central de qualquer estratégia D2C ou luxury digital.

O que ninguém disse à consumidora

A consumidora que envia uma selfie para receber um diagnóstico de pele *não pensa* que está enviando um dado biométrico irreversível, comparável legalmente à digital ou à íris. Ela pensa que está usando um filtro do Instagram. A indústria sabe que ela pensa assim. E construiu o produto contando com essa diferença de percepção.

Esta é a parte difícil. E é a parte que vai colapsar primeiro.

> O PROBLEMA SILENCIOSO
>
> O modelo atual depende de a consumidora *não compreender plenamente* o que ela está entregando. Qualquer movimento regulatório, jornalístico ou ativista que aumente essa compreensão derruba a base de confiança. E esses movimentos estão acontecendo simultaneamente em três continentes.

O paralelo com redes sociais — e por que ele assusta

A indústria de cosméticos está, em 2026, no ponto exato em que estavam Facebook e Cambridge Analytica em 2015: coletando massivamente, monetizando de forma opaca, com um risco reputacional acumulado que ninguém ainda precificou e com uma narrativa pública ainda favorável. O que veio depois — a queda de confiança, as audiências no Congresso, a regulação reativa — é instrutivo. **É evitável.**

A diferença é que cosméticos têm uma vantagem que redes sociais nunca tiveram: **a relação com a consumidora é, no fundo, sobre cuidado**. A marca pode escolher ser confiável de forma demonstrável. Pode escolher ser a primeira a dizer "nós não vemos". Esse movimento — feito a tempo — é diferenciação competitiva. Feito tarde, é crisis management.

> *"A pergunta para o conselho não é se a relação atual com o dado da consumidora é sustentável. É quanto tempo falta até ela parar de ser."*

CAPÍTULO II

O Cerco *Regulatório*.

Três continentes, três regulações, uma direção comum: o fim da era em que "consentimos com tudo" era uma defesa válida.

Existe um equívoco confortável compartilhado por boa parte da liderança jurídica das casas de cosméticos: o de que a regulação atual de dado, embora pesada, pode ser administrada com termos de uso bem escritos, banners de cookie, e um DPO competente. Esta visão é correta para 2022. Está errada para 2026.

LGPD — o artigo 11 que ninguém leu direito

A Lei Geral de Proteção de Dados brasileira classifica como **dado pessoal sensível**: dado biométrico, dado de saúde, dado genético, vida sexual. Selfie analisada para detectar oleosidade da pele e idade aparente cai em pelo menos duas categorias. Análise capilar com diagnóstico de queda cai em "saúde". DNA cosmético cai em "genético".

O artigo 11 exige que o tratamento desses dados ocorra **com consentimento específico e destacado** — não embutido em um termo de uso de 40 páginas — ou em hipóteses excepcionais (proteção da vida, tutela da saúde, etc.) que não cobrem operação comercial cosmética. A ANPD ainda não testou esses limites em casos de marca, mas *vai testar*, e o ônus da prova é da empresa.

GDPR — onde o regulador já se mexeu

O regulamento europeu é mais maduro e mais agressivo. As CNILs nacionais (França, Itália, Espanha) já multaram empresas de tecnologia em centenas de milhões por uso de dado biométrico sem base legal robusta. O caso Clearview AI — que treinou modelo facial em fotos públicas — gerou multas em série em quatro países. **Cosmético com selfie analisada é o próximo alvo natural**.

A Europa também aprovou o **AI Act**, com vigência escalonada até 2027. Sistemas de IA que processam dado biométrico para inferir características pessoais (idade, emoção, estado de saúde) estão classificados

como *alto risco*. Isto exige avaliação de conformidade, documentação técnica, supervisão humana, transparência. Custo de compliance estimado por sistema: **seis a sete dígitos**.

EUA, China e a fragmentação

Os Estados Unidos não têm lei federal, mas têm Illinois (BIPA), Texas, Washington — e a Califórnia com CCPA/CPRA. O BIPA já produziu acordos de bilhões contra Facebook e Google por uso de reconhecimento facial. **A jurisprudência é hostil.** A China, por outro lado, tem PIPL — uma das leis de proteção mais rigorosas do mundo, com transferência internacional de dado pessoal severamente controlada.

Para uma marca global, isto significa que a operação atual depende de manter **cinco ou seis arquiteturas regulatórias diferentes em paralelo**, cada uma com sua própria base legal, sua própria localização de dado, sua própria governança de consentimento. É insustentável operacional e financeiramente.

A virada conceitual: de minimização declarada para minimização provada

A direção que todas essas regulações estão tomando converge em um único princípio:

> *"Não basta dizer que o dado é minimamente usado. É preciso provar matematicamente que ele não pode ter sido usado de outra forma."*

É exatamente neste ponto que FHE deixa de ser curiosidade técnica e vira **vantagem regulatória estrutural**. Uma marca que processa selfie da consumidora *sob FHE* pode demonstrar à autoridade reguladora — e à imprensa — que o dado nunca foi visualizável pelo servidor, nunca foi armazenado em claro, nunca poderia ter sido visto por funcionário, nunca poderia ter vazado em breach. **Isto não é uma política. É um teorema.**

A JANELA ESTRATÉGICA

Reguladores estão buscando casos de uso "exemplares" para citar em decisões e diretrizes. A primeira marca global de cosméticos a apresentar arquitetura FHE auditável para análise facial vira *case oficial* da própria autoridade. Isto é proteção regulatória + posicionamento de marca em uma única jogada.

O custo de não agir, em números

RISCO	PROBABILIDADE 5 ANOS	IMPACTO TÍPICO
Multa GDPR/LGPD por base legal frágil	Alta	2–4% do faturamento global
Class action nos EUA por dado biométrico	Média-alta	US$ 100M–650M (precedentes BIPA)
Breach de imagem facial vazada	Média	Crise reputacional 18–36 meses
Bloqueio de feature por AI Act	Alta na UE	Perda de mercado regional
Consent fatigue → queda de conversão	Certa	Perda silenciosa, difícil de medir

CAPÍTULO III

FHE em Linguagem *Executiva*.

Sem matemática. Sem jargão. Apenas o que a alta gestão precisa entender para tomar uma decisão de US$ 10 milhões.

Imagine um cofre transparente. Você consegue ver que há algo dentro, mas não consegue ver o que é. Agora imagine que você consegue, de fora do cofre, com luvas mágicas, manipular o conteúdo: somar duas coisas que estão lá dentro, multiplicar, comparar. Você executa operações no conteúdo do cofre sem nunca abri-lo. Quando termina, devolve o cofre fechado para a dona da chave, que abre e vê o resultado. Isto é Criptografia Totalmente Homomórfica, em uma frase.

O salto conceitual

Toda a criptografia que sua empresa usa hoje — TLS no site, AES nos backups, HTTPS no app — protege o dado em *dois* dos três estados possíveis:

- **Em trânsito** — entre dispositivos. Resolvido por TLS.
- **Em repouso** — armazenado. Resolvido por AES nos discos.
- **Em uso** — quando o servidor processa. *Aqui o dado precisa estar em claro.*

O terceiro estado é o calcanhar de aquiles de toda arquitetura de privacidade da história. Quando o servidor calcula sua recomendação de creme, ele *precisa* ver sua selfie. Quando o algoritmo de scoring roda, ele *precisa* ver suas variantes genéticas. É nesse instante que o dado é vulnerável a funcionário desonesto, a invasão, a subpoena governamental, a backup mal-configurado, a log mal-rotacionado.

FHE elimina o terceiro estado. O servidor processa o dado **sem nunca ter acesso ao plaintext**. Esta é uma mudança de fase, não uma melhoria incremental.

Como funciona, em uma analogia que aguenta escrutínio

O mecanismo matemático real envolve reticulados (lattices) e o problema RLWE (Ring Learning With Errors) — que é o mesmo problema sobre o qual a próxima geração de criptografia pós-quântica é construída. Mas a intuição executiva é a seguinte:

> ANALOGIA
>
> A consumidora "tranca" sua selfie em uma caixa matemática usando uma chave que só ela tem. Envia a caixa fechada para o servidor da marca. O servidor — que *nunca* recebe a chave — executa todo o algoritmo de análise de pele *sobre a caixa fechada*, produzindo uma nova caixa que contém o resultado, ainda fechada. Devolve para a consumidora. Ela abre, vê o diagnóstico. Em nenhum momento da cadeia o servidor pôde ver a foto.

O que FHE oferece que nada mais oferece

TECNOLOGIA	O QUE PROMETE	O QUE FALHA
Anonimização	"Removemos o nome"	Re-identificação trivial; CNIL e ANPD já invalidaram
TEE (enclave de hardware)	"O chip isola"	Confia no fabricante; vários ataques laterais publicados
Federated Learning	"Dado fica no celular"	Gradientes vazam dado; já demonstrado em papers
Differential Privacy	"Adicionamos ruído"	Bom para estatística agregada, ruim para decisão individual
FHE	**"Servidor nunca vê em claro"**	**Custo computacional alto — mas decrescente**

FHE é a única tecnologia desta lista cuja garantia é **matemática e auditável por terceiro**, e não dependente de confiança em hardware, fornecedor ou política interna. Para um regulador, é a diferença entre "acreditar" e "verificar".

Os três sabores que importam

Existem três famílias principais de FHE em uso prático. A alta gestão não precisa decidir qual usar — o time técnico decide — mas precisa saber que existem, porque a escolha define o que é viável:

CKKS

APROXIMADO · NÚMEROS REAIS

O sabor para machine learning, análise estatística, processamento de imagem. Permite multiplicações e somas sobre vetores grandes. Lattigo e OpenFHE implementam.

BFV/BGV

EXATO · INTEIROS

O sabor para banco de dados cifrado, contagens, scoring exato. Quando o resultado precisa ser idêntico ao do plaintext.

TFHE

BOOLEANO · ULTRAFINO

Operações lógicas bit-a-bit, comparações, programas arbitrários. Mais lento por operação, mas o mais flexível. Concrete (Zama) é a referência.

Híbrido

NA PRÁTICA

Sistemas reais combinam dois ou três. Inferência facial em CKKS, scoring exato em BFV, decisões finais em TFHE.

O mito do custo: o que você precisa saber

O argumento padrão contra FHE é "é caro demais". Em 2018, isso era verdade — uma multiplicação cifrada custava milhões de vezes mais que uma multiplicação em claro. Em 2026, é uma meia-verdade que precisa ser desmontada com cuidado:

- **O custo caiu duas a três ordens de magnitude** em sete anos. A curva é constante e não mostra sinal de saturação.
- **Para inferência sobre imagem pequena** (224×224, modelo enxuto de visão para classificação de pele), latência hoje é de poucos segundos por consulta — comercialmente viável para diagnóstico que *não* precisa ser em tempo real.
- **Aceleradores de hardware** (Intel HEXL, FPGAs e ASICs específicos) estão chegando ao mercado e prometem outro 10–100× de redução de custo nos próximos 24 meses.
- **O modelo certo é seletivo**: usar FHE apenas no núcleo sensível (a foto, o DNA, o microbioma) e manter o resto da operação em texto claro. Isso reduz o custo total para uma fração do orçamento de TI atual.

O custo de FHE não é uma barreira. É uma **variável de design**. A pergunta não é "podemos pagar?" — é "para qual caso de uso o ROI já fecha hoje?". E a resposta, como o próximo capítulo mostra, é: vários.

CAPÍTULO IV

Casos de Uso por *Linha*.

O que muda, concretamente, em cada vertical da operação cosmética. Skincare, makeup, haircare, fragrância, wellness, derma e luxo — cada uma com sua oportunidade específica.

Skincare — o caso âncora

Skincare é o terreno mais óbvio porque é onde a coleta de dado biométrico já está mais avançada. As marcas que rodam apps com análise facial diária — La Roche-Posay Effaclar Spotscan, Vichy SkinConsult, Olay Skin Advisor, Neutrogena Skin360 — coletam, hoje, em volume industrial, fotos de rosto da própria base de clientes premium.

Casos de uso FHE na linha skincare:

1. DIAGNÓSTICO DE PELE SEM ENVIO DE SELFIE

Um modelo de visão mobile (MobileNet-V3 ou equivalente, ~2.5M de parâmetros) roda *localmente no celular*, em claro, e converte a selfie em um embedding de 256 dimensões — um vetor numérico que captura poros, oleosidade, manchas, textura, idade aparente. A imagem original nunca sai do celular. Apenas o embedding é cifrado e enviado. O servidor executa o classificador linear final (scoring dos produtos do catálogo) sobre o embedding cifrado, devolve o ranking cifrado, e a consumidora decifra localmente. **A marca nunca vê o rosto nem o embedding em claro — é o padrão real usado por L'Oréal SkinConsult, Vichy Effaclar e Olay Skin Advisor.**

2. ACOMPANHAMENTO LONGITUDINAL SEM ÁLBUM DE FOTOS NO SERVIDOR

O grande valor de skincare é o "antes e depois" de 90 dias. Hoje, isso significa que a marca tem um *álbum cifrado em repouso, mas que precisa ser decifrado para comparar*. Com FHE, a comparação acontece sob cifra. O servidor calcula o delta sem ver nenhuma das duas fotos.

3. VALIDAÇÃO CIENTÍFICA DE EFICÁCIA (CLAIMS DEFENSÁVEIS)

"Reduz rugas em 28% após 4 semanas" — esse claim precisa ser sustentado por estudo com painel de consumidoras reais. O painel envia fotos antes e depois. A análise é feita sob FHE. O resultado agregado

é publicado, mas **nenhuma foto individual jamais foi acessada** — nem pela marca, nem pelo lab terceirizado, nem pelo regulador. Isto é um claim impossível de contestar por argumento de privacidade.

Makeup — o "try-on" sem o vampiro de imagem

A maquiagem virtual (try-on AR) é um dos canais de conversão mais poderosos do beauty digital. Mas é também um dos mais agressivos em coleta facial. Cada experimentação envolve mapeamento facial 3D, e na maioria das implementações esse mapeamento é processado em servidor.

Caso FHE: **try-on cifrado no edge**. O modelo de detecção de landmarks roda em parte no celular (em claro, no dispositivo da própria usuária — sem problema legal) e em parte no servidor sob cifra (a aplicação dos pigmentos virtuais, a renderização). A marca recebe métricas de engajamento agregadas e cifradas: "X usuárias provaram batom Y", sem saber quem ou quando individualmente, sem armazenar imagens.

Valor adicional: **elimina o problema chinês**. Try-on AR em mercado chinês hoje exige enviar dado biométrico para servidor doméstico (lei PIPL). FHE quebra essa exigência porque o dado nunca está em claro em lugar nenhum.

Haircare — diagnóstico capilar e a sensibilidade subestimada

Foto de couro cabeludo é dado de saúde. Padrão de queda capilar é dado clínico. A marca de haircare que faz diagnóstico via foto — categoria em forte expansão (Function of Beauty, Prose, Living Proof) — está processando dado de saúde sob disfarce de personalização.

Casos FHE:

- **Análise de couro cabeludo sem envio de foto** — CNN mobile local extrai embedding da foto (em claro, no celular); apenas o embedding é cifrado e enviado ao servidor, que executa o classificador final (caspa, oleosidade, alopecia incipiente) sob cifra.
- **Match com dermatologista parceiro sem ver dado** — a marca pode oferecer "consulta com derma" como upsell, com a derma vendo a foto decifrada com chave da paciente, e a marca nunca vendo nada além da métrica de conversão.
- **Acompanhamento de tratamento** em 6 meses sem armazenar histórico fotográfico em servidor da marca.

Fragrância — o caso menos óbvio, mas talvez o mais elegante

Perfume parece estar fora desta discussão — não há foto, não há genoma. Mas perfume é, há mais de uma década, um dos produtos com **perfilamento emocional mais profundo** da indústria. Marcas de luxo (Chanel, Guerlain, Dior, Frédéric Malle) sabem que escolha de fragrância correlaciona com personalidade, estado emocional, estação da vida, vínculos afetivos. Quizzes online de "qual perfume é para você" são, na prática, instrumentos de psicometria.

Caso FHE: **quiz emocional sob cifra**. A consumidora responde 30 perguntas íntimas sobre memória, lugar, emoção. As respostas são cifradas. O motor de match roda sobre as respostas cifradas. Devolve a recomendação cifrada. **A marca nunca sabe que esta cliente associa "casa" a "ausência da mãe"** — embora o algoritmo tenha usado essa informação para recomendar a fragrância certa.

Por que isto é elegante: o luxo de fragrância vende intimidade. "*Nós entendemos sua alma sem vê-la*" é um manifesto de marca que custa zero em produção e vale milhões em narrativa.

Wellness, beauty supplements e ingestáveis

A categoria de "beauty from within" — colágeno, biotina, ácido hialurônico oral, suplementos para pele e cabelo — é a que mais cresce no setor. E é a que mais se aproxima de farmacêutica sem ter os controles de farmacêutica. Tipicamente envolve coleta de dado de dieta, sono, ciclo, sintomas, medicamentos em uso.

Caso FHE: **recomendação de suplementação personalizada sem prontuário no servidor**. O usuário entra com seus dados de saúde no celular. A análise de adequação (incluindo verificação de interação com medicamentos declarados) roda sob cifra. A marca recebe a venda; nunca recebe o prontuário.

Valor regulatório enorme: este caso de uso elimina o risco de a marca ser reclassificada pela ANVISA/FDA como "operação de saúde".

Linha derma — onde FHE é quase mandatório

Dermocosmético é a fronteira que mais escorrega de "cosmético" para "tratamento". La Roche-Posay, Vichy, Eucerin, Avène, CeraVe — marcas que vendem como cosmético mas operam como adjuvante terapêutico. Quando essas marcas oferecem teleconsulta com derma, ou diagnóstico assistido por IA, estão operando como produto de saúde com regulação de cosmético. Esse arbitrage está acabando.

FHE permite que essas marcas ofereçam serviços de nível clínico **sem assumir o passivo legal de operação de saúde**, porque a marca nunca vê o dado clínico. A derma parceira vê. O paciente vê. A marca nunca.

Luxo e ultra-luxo — o argumento de exclusividade

Para Chanel, Hermès, La Mer, La Prairie — marcas onde o cliente paga prêmio de 10×–30× sobre o equivalente mass — privacidade vira **parte do produto**, não suporte ao produto. O cliente de ultra-luxo já paga por discrição em outros setores (private banking, aviação executiva, joalheria sob medida). FHE traz essa lógica para beauty.

> **POSICIONAMENTO ESTRATÉGICO**
>
> O ultra-luxo é o melhor lugar para começar. O cliente entende valor de discrição. O preço comporta o overhead computacional de FHE. A narrativa é diferenciação genuína. E o caso de sucesso aqui se torna o template para escalar para o mass premium nos anos seguintes.

R&D colaborativo — o caso B2B que ninguém vê

Fora dos casos voltados ao consumidor, há um caso interno gigantesco: **colaboração entre marca, fornecedor de ativos e laboratório de teste**. Cada uma das três tem propriedade intelectual que não quer entregar às outras. Hoje isso é mediado por NDAs e por boa-fé. Com FHE, a colaboração vira matemática:

- O fornecedor de ativos cifra a composição do princípio ativo proprietário.
- A marca cifra o briefing de formulação.
- O lab cifra o protocolo de teste.
- O resultado — eficácia, segurança, estabilidade — é computado sob cifra e revelado apenas como métrica final.

Nenhuma das três partes vê os ativos das outras. Isto destrava colaborações que hoje não acontecem por desconfiança mútua.

Estudos de painel sem o painel ver a si mesmo

Painel de consumidoras para estudo de eficácia é caro, lento, e juridicamente carregado. Com FHE, cada participante contribui dados cifrados. As estatísticas são computadas sob cifra. O resultado publicado tem exatamente o mesmo valor científico, sem nenhuma das contradições éticas atuais. Isto também vale para estudos antropométricos, pesquisas de mercado profundas, e segmentação psicográfica.

CAPÍTULO V

A Economia do *Espelho Cego*.

Os números reais. Quanto custa, quanto retorna, e onde o capital encontra o valor.

Toda decisão de investimento em alta gestão precisa passar por três peneiras: capex, opex recorrente, e valor presente líquido descontado a um custo de capital realista. FHE não é exceção — e merece ser analisado com o mesmo rigor que qualquer outro investimento de transformação digital. O que segue é uma estimativa por ordem de magnitude, calibrada para uma marca global de cosméticos com receita entre US$ 1B e US$ 10B.

O custo de fazer (capex inicial)

COMPONENTE	INVESTIMENTO TÍPICO
Time fundador (1 cripto-engenheiro sênior, 2 ML eng, 1 PM, 1 jurídico de privacidade)	US$ 1.2M – 2M / ano
Licenças e tooling (Lattigo open, Concrete commercial tier, OpenFHE)	US$ 50k – 250k / ano
Infra: GPUs e CPUs com AVX-512 ou aceleradores (HEXL, FPGA opcional)	US$ 300k – 800k inicial
Consultoria estratégica (Zama, Duality, Inpher) para arquitetura inicial	US$ 200k – 500k
Estudo regulatório com escritório especializado (privacidade + saúde)	US$ 150k – 400k
Total ano 1	**US$ 2M – 4M**

O custo de operar (opex anual recorrente)

Após estabilização, uma operação FHE em produção para um caso de uso central (digamos, análise facial cifrada para 5 milhões de consultas/mês) tem opex dominado por:

ITEM	ESTIMATIVA ANUAL
Compute (FHE é 100×–1000× mais caro que plaintext na operação central)	US$ 800k – 2.5M
Time de manutenção (4–6 engenheiros)	US$ 1.5M – 2.5M
Auditoria de segurança e conformidade externa (anual)	US$ 200k – 500k
Opex anual estabilizado	**US$ 2.5M – 5.5M**

Para uma marca com receita acima de US$ 2B, isto representa entre **0,1% e 0,3% do faturamento**. Para colocar em perspectiva: é menos do que a maioria das marcas gasta em *uma única campanha de relançamento de hero product*.

O retorno — onde o dinheiro reaparece

O ROI de FHE não vem de redução de custo. Vem de cinco vetores que precisam ser modelados separadamente:

1. Redução de risco regulatório (valor segurador)

A exposição esperada a multas GDPR/LGPD/BIPA, em cenário base de uma marca global processando dado biométrico, é estimada em **US$ 30M–150M de valor presente esperado em 5 anos**. FHE não elimina o risco mas reduz a magnitude e a probabilidade em ambos os fatores. Tratamento como hedge, com desconto de 40–60%, gera valor segurador na faixa de **US$ 12M–80M**.

2. Habilitação de receita nova (valor opcional)

Mercados que hoje estão fechados ou são frágeis: cosmético genético, microbioma, derma com IA, beauty wellness. Cada um destes é um mercado de US$ 500M–5B endereçável globalmente. FHE

habilita participação defensável em todos eles. **Valor opcional estimado: US$ 50M–300M ao longo de 5 anos**, com probabilidade de captura entre 5% e 30%.

3. Prêmio de marca (valor narrativo)

Este é o vetor mais difícil de quantificar e o mais provável de surpreender para cima. A diferença entre uma marca premium e uma commodity é, em última análise, narrativa. "*Nós nunca vemos seu rosto*" é uma linha de comunicação que sustenta uma campanha global por dois anos sem perder relevância. Comparáveis: o "Privacy. That's iPhone." da Apple é estimado por analistas em **US$ 8B–15B de valor de marca incremental**. Cosmético em escala menor, mas o efeito multiplicador é o mesmo.

4. Vantagem em parcerias estratégicas (valor de moat)

Hospitais, clínicas dermatológicas, plataformas de telemedicina, cadeias de farmácia estão cada vez mais cautelosos em parcerias que exijam compartilhamento de dado de paciente. Marcas com capacidade FHE viram parceiras viáveis em situações onde concorrentes não podem entrar. **Vale 2–4 parcerias estratégicas exclusivas em 36 meses**, cada uma com valor presente estimado em US$ 5M–25M.

5. Redução do custo de consent fatigue (valor silencioso)

Consumidoras estão cada vez menos dispostas a clicar "aceito" em termos de uso. Conversão de funis que exigem consentimento explícito de dado biométrico já caiu 15–35% nos últimos 24 meses na maioria das plataformas medidas. Uma proposta que *elimina a necessidade de consentimento robusto* porque o dado nunca é "tratado" no sentido legal traz uplift de conversão direto. **Em volumes da indústria, ponto percentual de conversão vale dezenas de milhões.**

O caso de negócio resumido

~US$ 3M INVESTIMENTO ANO 1	~US$ 4M OPEX ANUAL ESTABILIZADO
US$ 80M+	10×–30×

VALOR SEGURADOR + OPCIONAL (5 ANOS)

ROI ESPERADO EM HORIZONTE 5 ANOS

> *“Em qualquer modelagem honesta, FHE para uma marca global de cosméticos é o investimento de transformação digital com melhor relação assimetria-de-retorno disponível em 2026.”*

Não porque seja certeza de retorno alto. Mas porque o downside é limitado (custo conhecido, perfeitamente orçável) e o upside é estruturalmente assimétrico — combinando hedge regulatório, habilitação de receita, narrativa de marca e vantagem de parceria em uma única jogada.

CAPÍTULO VI

Vantagem Competitiva e *Posicionamento*.

FHE é, antes de tudo, narrativa. E narrativa, em beauty, é o produto.

Há um erro frequente em conversas de adoção de tecnologia em conselhos de marca: tratar a tecnologia como uma melhoria operacional. CRM melhor, supply chain mais eficiente, atendimento mais rápido. FHE não pertence a essa categoria. FHE pertence à categoria de tecnologias que mudam a **história que a marca pode contar** — e em beauty, a história é o produto.

O paralelo com Apple e a privacidade

Em 2014, a Apple estava perdendo terreno para o Android em features funcionais. Câmeras melhores, telas maiores, assistentes mais inteligentes — todos ficavam para trás. A resposta da Apple não foi competir em features. Foi escolher um vetor onde os competidores **não podiam responder**: privacidade. Não porque a Apple fosse intrinsecamente mais ética, mas porque seu modelo de negócio (vender hardware caro) era estruturalmente compatível com não monetizar dado, enquanto o de Google e Facebook não era.

Foram dez anos de campanhas, eventos, anúncios em outdoor, slogans simples. "*What happens on your iPhone, stays on your iPhone.*" O resultado: um diferencial competitivo que sobrevive a três gerações de produto e que se transformou em **fosso de marca medido em centenas de bilhões de dólares**.

O mesmo movimento está disponível para uma — exatamente uma — casa de cosméticos hoje. A primeira a fazê-lo trava a posição. A segunda parece imitação. A terceira parece desespero.

Por que cosmético é o setor mais bem posicionado para esta narrativa

Quatro razões estruturais:

1. **A relação com a consumidora é íntima.** Beauty é o setor B2C mais próximo do corpo, da identidade, da auto-imagem. Privacidade não é uma feature — é uma extensão natural da promessa de cuidado.
2. **O cliente premium paga por discrição.** Em outros setores onde o cliente paga prêmio (private banking, aviação executiva, alta joalheria), discrição é parte central do serviço. Beauty premium ainda não capturou isso.
3. **A competição não está olhando.** Praticamente nenhum dos times de IA e CDO das grandes casas tem cripto-engenheiro sênior. Há uma janela de 18–36 meses em que o investimento é desproporcionalmente fácil.
4. **O regulador está procurando casos exemplares.** A primeira marca a apresentar arquitetura FHE auditável vira citação em diretriz. Isto é proteção dupla — competitiva e regulatória.

Os três posicionamentos possíveis

Posicionamento 1 — A Marca Que Não Vê

Foco em diferenciação narrativa pura. Campanha global construída em torno do conceito de privacidade matemática. Preço idêntico ou próximo dos concorrentes; o valor extraído é em market share, não em margem. Funciona melhor para mass premium e digital nativo.

Posicionamento 2 — O Luxo Verdadeiro É Discrição

Foco em ultra-luxo. Privacidade vira parte do produto, não do marketing. Preço sustenta o overhead. Cliente entende o valor sem precisar que seja explicado. Funciona para casas como Chanel, Hermès, La Mer, La Prairie, Guerlain.

Posicionamento 3 — O Padrão de Indústria

Foco em liderar consórcio aberto. A marca contribui para padronização (talvez via IFSCC ou similar), publica papers, participa de regulação. Ganha posição de autoridade técnica e moral sobre o setor. Funciona melhor para o player #1 ou #2 globais que querem entrincheirar-se.

Os três não são mutuamente exclusivos. Uma estratégia robusta combina o posicionamento 2 (no portfolio premium) com o posicionamento 3 (no nível de grupo). O posicionamento 1 fica para a marca digital nativa do portfolio.

O custo de não posicionar

Há um cenário que precisa ser explicitado em conselho: o que acontece se nenhuma das grandes casas adotar FHE nos próximos 36 meses?

Resposta: **uma marca pequena, digital nativa, vai fazê-lo**. E vai capturar a narrativa inteira por uma fração do custo. Não estará vendendo R$ 800 em creme — estará vendendo R$ 200 em creme com a mesma promessa. As consumidoras de Gen Z e Alpha, que decidem por valores, vão migrar. Em 5 anos, o que era posicionamento de luxo vira commodity, e a marca pequena vira o caso de sucesso citado em todos os reports da McKinsey e BCG sobre o futuro do beauty.

> *“A escolha não é entre adotar FHE ou não. É entre liderar a narrativa ou comprá-la a múltiplos elevados depois.”*

CAPÍTULO VII

Roadmap de *24 Meses*.

Da decisão do conselho ao primeiro produto público. Quatro fases, marcos claros, métricas de saída em cada uma.

01

MESES 1–6 · APRENDER

Fundação e capacidade interna

Contratar o cripto-engenheiro sênior fundador. Esta contratação é o gargalo real — há talvez 200 pessoas no mundo qualificadas, e o trabalho é convencer uma delas a sair de Zama, Duality, Inpher, IBM Research, Google Brain, ou de uma cadeira acadêmica. Orçamento de aquisição: US$ 400k–700k pacote total.

Em paralelo: contratar consultoria estratégica com Zama ou Duality para arquitetura inicial. Reproduzir benchmarks públicos (Lattigo CIFAR cifrado, OpenFHE logistic regression). Identificar três casos de uso candidatos com ROI claro e elegê-los para piloto.

Métrica de saída: arquitetura técnica documentada, três casos selecionados, parecer jurídico interno sobre LGPD/GDPR/AI Act validando viabilidade.

02

MESES 7–14 · CONSTRUIR

Piloto interno em ambiente controlado

Construir um único caso de uso, ponta a ponta, em ambiente controlado interno. Recomendação: análise facial cifrada para classificação de tipo de pele (categórico, baixa dimensionalidade, modelo enxuto). Isto é tecnicamente o mais maduro e o de maior valor narrativo.

Validar latência (alvo: <3s por consulta), custo (alvo: <US$ 0,01 por consulta após otimização), precisão (alvo: dentro de 2% do modelo equivalente em plaintext), e fluxo de chaves (alvo: chave nunca sai do dispositivo da consumidora).

Em paralelo: começar a construir o storytelling. Briefing com agência de marca. Workshop com diretor criativo. Não anunciar ainda.

Métrica de saída: demo funcional em ambiente de produção paralelo, métricas validadas por terceiro independente, narrativa de marca pré-aprovada por CEO/CMO.

03

MESES 15–20 · LANÇAR BETA

Programa fechado com clientes reais

Lançar para um grupo seleto de clientes — idealmente 5.000 a 50.000 — em um único mercado. Sugestão: lançar primeiro em mercado europeu, onde a narrativa de privacidade ressoa mais forte e onde o regulador é mais sofisticado para entender o valor.

Documentar tudo. Iterar arquitetura. Medir conversão, NPS, dwell time, e — a métrica decisiva — diferença de comportamento entre o grupo FHE e o grupo de controle (mesma feature, pipeline tradicional).

Em paralelo: começar a falar com auditores externos para certificação de conformidade. Engajar reguladores em conversas informais. Preparar caso para apresentação em IFSCC, in-cosmetics, Cosmoprof.

Métrica de saída: validação comercial mensurável, certificação de conformidade externa, primeira menção pública controlada (em conferência técnica, não em campanha de marca ainda).

04

MESES 21–24 · ANUNCIAR

Lançamento global e captura de narrativa

Campanha global. Manifesto de marca. Evento de imprensa em Paris ou Nova York. Whitepaper técnico aberto. Convite à imprensa para auditar a arquitetura. Conversa com reguladores principais. Posicionamento como referência setorial.

Esta é a fase em que o investimento dos 20 meses anteriores é monetizado em narrativa. Feito corretamente, gera 18–36 meses de cobertura editorial, 2–3 anos de vantagem competitiva narrativa, e uma posição regulatória defensável.

Métrica de saída: reconhecimento de marca, cobertura, citação em diretrizes regulatórias, e — o teste final — concorrentes anunciando "iniciativas similares" 6–12

meses depois.

Marcos que o conselho deve cobrar

MARCO	QUANDO	COBRANÇA
Cripto-engenheiro fundador contratado	Mês 3	Sem isto, não há projeto
Caso de uso selecionado e validado por jurídico	Mês 6	Sem alinhamento, atrito eterno
Demo técnica funcional	Mês 12	Prova de viabilidade real
Métricas de piloto validadas por terceiro	Mês 18	Defesa contra "isto é só hype"
Lançamento público com narrativa	Mês 24	O retorno do investimento começa aqui

CAPÍTULO VIII

Riscos, Mitigações e *Armadilhas*.

O que pode dar errado, em ordem decrescente de probabilidade e gravidade.

Risco 1 · Não conseguir contratar o talento fundador

Probabilidade: alta. **Impacto:** bloqueante.

Há talvez 200 pessoas no mundo qualificadas a liderar uma operação de FHE em produção. A maioria está em poucas empresas (Zama, Duality, Inpher, IBM Research, Google) ou na academia. A maioria nunca pensou em trabalhar para cosméticos.

Mitigação: tratar como contratação de C-level, não de engenheiro. Pacote de equity, autonomia técnica, missão clara. Considerar aquisição de uma startup (acquihire) como atalho — Zama, Optalysys, Inpher já recebem ofertas regulares; o caminho de aquisição parcial existe.

Risco 2 · Custo computacional não cair na velocidade prevista

Probabilidade: média. **Impacto:** manageable.

A curva de redução de custo de FHE depende de avanços algorítmicos e de hardware. Se o ritmo desacelerar, o caso de uso pode ser viável apenas para produtos premium com volume baixo, não para mass.

Mitigação: começar o portfolio pelo segmento ultra-luxo, onde o custo já fecha hoje. Escalar para mass apenas quando a economia permitir. Em qualquer cenário, o caso premium se sustenta sozinho.

Risco 3 · Regulador interpreta a feature como insuficiente

Probabilidade: baixa. **Impacto:** alto.

Há uma chance pequena de que ANPD, CNIL ou ICO entendam que mesmo com FHE, o ato de cifrar e enviar dado biométrico para o servidor já configura "tratamento" no sentido legal. Isto seria uma

interpretação minoritária, mas possível.

Mitigação: engajar o regulador **antes** do lançamento, em modo consultivo. Apresentar a arquitetura. Buscar parecer prévio (na UE, mecanismo formal; no Brasil, informal mas possível). Publicar a arquitetura aberta para revisão acadêmica. Esta é uma decisão jurídica com upside enorme: o regulador que opina favoravelmente vira aliado.

Risco 4 · Concorrente anuncia primeiro

Probabilidade: média. **Impacto:** alto.

L'Oréal, Estée Lauder, Shiseido, Unilever, P&G — qualquer um pode estar com projeto similar em curso. Improvável, mas possível. Se acontecer, o segundo a chegar perde a maior parte do prêmio narrativo.

Mitigação: velocidade. Cada mês de atraso é um mês a mais de exposição ao risco. Considerar parceria com vendor de FHE como aceleração (Zama Concrete, Duality Confidential AI) em vez de construir tudo do zero. Custo maior, mas time-to-narrative significativamente menor.

Risco 5 · A narrativa não ressoa com o consumidor

Probabilidade: média-baixa. **Impacto:** médio.

Existe a possibilidade de que a consumidora simplesmente não se importe — que a fadiga de privacidade tenha levado todo mundo a parar de prestar atenção a estas mensagens.

Mitigação: testar a narrativa antes da campanha. Focus groups, A/B testing em cópia digital, mensuração de sentiment. Posicionar a feature como qualidade adicional do produto, não como manifesto isolado. Em pior caso, a feature ainda gera valor regulatório e operacional.

Risco 6 · Vulnerabilidade descoberta no esquema FHE

Probabilidade: muito baixa. **Impacto:** alto.

Esquemas FHE modernos (CKKS, BFV, BGV, TFHE) são baseados em problemas de reticulado bem estudados — os mesmos problemas sobre os quais NIST padronizou a próxima geração de criptografia pós-quântica (ML-KEM, ML-DSA). A confiança matemática é alta. Mas avanços teóricos imprevistos sempre são possíveis.

Mitigação: usar parâmetros conservadores. Acompanhar a literatura. Ter plano de migração entre esquemas (a arquitetura deve ser desacoplada do esquema específico). Não usar FHE como única camada de defesa — combinar com TLS, AES, segregação de chaves.

Armadilha 1 · Tratar como projeto de TI

O erro mais comum em adoção de tecnologia narrativa é colocá-la sob o CIO/CTO em vez de sob CMO/CDO/CEO. Isto resulta em entrega técnica perfeita e narrativa morta. **FHE deve reportar ao CEO ou a um patrocinador de nível C com mandato amplo.**

Armadilha 2 · Comunicar cedo demais

Anunciar antes de ter produto funcional gera duas piores resultados possíveis: (a) competidores adaptam estratégia e neutralizam; (b) imprensa testa e descobre que ainda não está pronto. Comunicação só após validação independente.

Armadilha 3 · Esquecer a chave

FHE protege durante a computação. Mas o gerenciamento de chaves do lado da consumidora é onde a maioria das implementações falha. Se a chave está no cloud da marca, FHE perdeu o sentido. Se está no celular sem backup, perda de telefone = perda de histórico. **O design do gerenciamento de chave é metade do projeto.**

CAPÍTULO IX · MANIFESTO

Uma carta para a próxima década do *beauty*.

Para os CEOs, conselheiros e diretores criativos das casas que ainda podem escolher liderar.

A indústria que vocês lideram foi construída sobre uma promessa antiga: a de que o cuidado com a beleza é, no fundo, um cuidado com a pessoa. Que vender um creme, um perfume, um batom é vender uma forma de relação consigo mesma. Que a marca está do lado da consumidora — não contra ela, não acima dela, não sobre ela, mas *com* ela.

Esta promessa atravessou um século. Sobreviveu a guerras mundiais, revoluções culturais, ascensão do feminismo, queda do consumo conspícuo, ascensão do digital. Ela sobreviveu porque era — e em grande parte ainda é — verdadeira. As mulheres e homens que escolhem comprar de uma casa têm uma relação afetiva real com essa casa. Eles confiam.

Mas nos últimos cinco anos, sem que ninguém tenha decretado, a relação mudou de natureza. A consumidora deixou de ser quem entrega dinheiro e recebe produto. Tornou-se quem entrega dado biométrico, dado comportamental, dado emocional, e em alguns casos dado genético — e recebe produto, sim, mas também recebe uma exposição que ela não pediu, não compreende em profundidade, e que nenhum termo de uso sincero conseguiria explicar a tempo.

Esta mudança não foi causada por má fé. Foi causada por incremento. Cada feature acrescentou um pouco de coleta. Cada campanha pediu um pouco mais de personalização. Cada CRM tinha um pouco mais de campos. Em algum momento, sem decreto, sem manifesto, a relação atravessou uma fronteira ética que nenhum executivo individual conscientemente cruzaria.

É possível voltar atrás. Mais que isso: é estrategicamente preferível voltar atrás. Não porque a regulação exija — embora exija. Não porque o regulador esteja olhando — embora esteja. Mas porque **a relação original com a consumidora era mais valiosa**. Era mais durável. Era a base sobre a qual se construiu toda a narrativa de marca que ainda hoje sustenta o setor.

FHE — Criptografia Totalmente Homomórfica — é a primeira tecnologia em décadas que permite voltar atrás **sem perder as features**. É possível continuar oferecendo análise facial, recomendação personalizada, diagnóstico capilar, fragrância sob medida, suplemento customizado. É possível continuar

fazendo tudo o que a indústria descobriu fazer com dado nos últimos dez anos. **É possível fazer tudo isso sem nunca ver o dado.**

Esta frase parece, em uma primeira leitura, paradoxal. Em uma segunda leitura, parece técnica demais. Em uma terceira, parece o argumento mais óbvio que a indústria já teve à sua disposição. Como é possível recomendar um creme sem ver a pele? A matemática responde — e a resposta é elegante, antiga, e finalmente viável em produção.

O que está em jogo não é uma feature técnica. É a possibilidade de uma marca dizer, com verdade matemática e não com promessa de gestão: "*nós cuidamos de você sem invadir você*". É a possibilidade de oferecer cuidado sem extrair vigilância. É a possibilidade de devolver à consumidora a dignidade de não precisar escolher entre personalização e privacidade.

Esta possibilidade está aberta, hoje, para exatamente uma marca. A primeira a entender o que está em suas mãos. A primeira a contratar a engenheira certa, a chamar o jurídico certo, a apresentar o caso ao conselho certo. A primeira a publicar o whitepaper, a fazer a campanha, a defender a posição em entrevista, a sustentar a narrativa por dois anos seguidos sem ceder à tentação de diluir a mensagem.

Em três anos, esta posição vai estar tomada. A pergunta que precisa ser feita, em cada conselho que ainda tem o privilégio de escolher, é simples:

> *“Vamos ser quem disse primeiro, ou quem teve que explicar depois por que demorou tanto?”*

Há uma janela. É curta. É real. É historicamente rara. Indústrias inteiras passam décadas esperando por janelas como esta — e a maioria das casas nelas instaladas as perdem por excesso de prudência operacional. Cosméticos já passou por uma dessas janelas com o digital (e a maioria das casas perdeu para D2C nativas). Já passou por outra com sustentabilidade (e algumas casas usaram para se redefinir, outras só fizeram greenwashing). Esta é a próxima. É possivelmente a última desta década com capacidade de redefinir a narrativa central da indústria.

Quem ler este eBook tem em mãos um mapa. O mapa não é completo, não é sem riscos, não é sem custos. Mas é claro. E está, neste momento, na frente das pessoas certas para tomar a decisão certa.

O resto é coragem.

— Fim do Volume I

APÊNDICE A

Glossário *Executivo*.

Os termos que você vai ouvir do CTO. Em português direto.

FHE — FULLY HOMOMORPHIC ENCRYPTION

Criptografia que permite executar cálculos sobre dados cifrados sem descriptografá-los. O resultado, ao ser descriptografado, é igual ao que seria obtido sobre os dados originais.

RLWE — RING LEARNING WITH ERRORS

O problema matemático sobre o qual a maioria dos esquemas FHE modernos se baseia. É o mesmo problema da criptografia pós-quântica padronizada pelo NIST (ML-KEM, ML-DSA). Resistente tanto a computadores clássicos quanto quânticos.

CKKS

Esquema FHE para números reais com aritmética aproximada. O melhor para machine learning, análise estatística, processamento de imagem.

BFV / BGV

Esquemas FHE para inteiros com aritmética exata. Usados quando o resultado precisa ser idêntico ao do plaintext — banco de dados cifrado, scoring, contagens.

TFHE

Esquema FHE booleano e bit-a-bit. Mais lento por operação, mas o mais flexível — permite executar programas arbitrários sob cifra.

BOOTSTRAPPING

A operação que permite "reduzir o ruído" acumulado em um cálculo FHE, possibilitando computações de profundidade ilimitada. É a operação mais cara em FHE, e a maior parte do esforço de otimização concentra-se aqui.

PSI — PRIVATE SET INTERSECTION

Protocolo derivado de FHE/MPC que permite duas partes descobrirem a interseção de seus conjuntos sem revelar o restante. Útil para "quem é cliente em comum" sem revelar bases.

TEE — TRUSTED EXECUTION ENVIRONMENT

Tecnologia alternativa baseada em hardware (Intel SGX, AMD SEV-SNP). Confia no fabricante. FHE é matematicamente mais forte; TEE é hoje mais rápido.

MPC — MULTI-PARTY COMPUTATION

Outra tecnologia alternativa baseada em protocolos colaborativos entre múltiplas partes. Funciona, mas exige todas as partes online; FHE permite operação assíncrona.

LATTIGO

Biblioteca FHE em Go, mantida pela Tune Insight (spin-off do EPFL). Maturidade alta, código limpo, boa para integração em produtos comerciais.

OPENFHE

Biblioteca open-source em C++, sucessora de PALISADE. Mantida pela Duality Technologies. A mais completa em variedade de esquemas suportados.

CONCRETE

Framework FHE da Zama (Paris). Foco em TFHE e em facilidade de uso para desenvolvedores não-criptógrafos. Tem versão comercial.

APÊNDICE B

Fornecedores e *Talento*.

Onde está a capacidade comercial e onde estão as pessoas.

Fornecedores comerciais

VENDOR	SEDE	FOCO
Zama	Paris	TFHE, Concrete framework, foco em developer experience
Duality Technologies	EUA / Israel	OpenFHE, foco em saúde e finanças, consultoria pesada
Inpher	Suíça / EUA	FHE + MPC híbrido, foco em finanças e saúde
Tune Insight	Suíça (EPFL)	Lattigo, foco em pesquisa médica federada
Optalysys	Reino Unido	Aceleração óptica de FHE; hardware específico
Cornami	EUA	Aceleradores de hardware FHE
Fhenix	Israel	FHE em blockchain; menos relevante para cosmético

Centros acadêmicos onde mora o talento

- **EPFL (Lausanne)** — laboratório do Christian Cachin / Jean-Pierre Hubaux, origem do Lattigo
- **IBM Research** — origem histórica do FHE (Craig Gentry, 2009), continua produzindo papers

- **Microsoft Research** — biblioteca SEAL, Kim Laine
- **NJIT / Duality** — Yuriy Polyakov, Kurt Rohloff
- **Université Paris-Saclay / ENS** — Léo Ducas, várias contribuições centrais
- **KU Leuven (COSIC)** — Frederik Vercauteren
- **Stanford / MIT / CMU** — vários pesquisadores ativos, especialmente em ML+FHE

Bibliotecas open-source para o time técnico avaliar

- **Lattigo** (Go) — github.com/tuneinsight/lattigo
- **OpenFHE** (C++) — github.com/openfheorg/openfhe-development
- **Concrete** (Rust + Python) — github.com/zama-ai/concrete
- **SEAL** (C++) — github.com/microsoft/SEAL
- **HElib** (C++) — github.com/homenc/HElib

APÊNDICE C

30 Perguntas para o *CTO*.

A lista que você deveria levar para a próxima reunião com seu time técnico.

Estratégia e capacidade

1. Temos no time alguém com background em criptografia de reticulados? Se não, qual o plano de aquisição?
2. Qual é nossa exposição atual a tratamento de dado biométrico, em volume e em jurisdição?
3. Quais features do nosso produto, hoje, dependem de processar dado pessoal sensível em servidor?
4. Temos um inventário atualizado de quais dados saem do dispositivo da consumidora e onde são processados?
5. Qual é nosso parecer jurídico atual sobre a sustentabilidade dessa arquitetura nos próximos 36 meses?

Arquitetura técnica

6. Qual esquema FHE faz mais sentido para nosso primeiro caso de uso? CKKS, BFV, TFHE, ou híbrido?
7. Qual é a profundidade multiplicativa máxima do nosso modelo de inferência atual?
8. Conseguimos rodar nosso modelo de classificação de pele em FHE com latência aceitável hoje?
9. Qual seria o overhead computacional estimado, em ordem de magnitude, para nosso caso?
10. Como pretendemos gerenciar chaves do lado da consumidora? Backup? Recuperação?
11. O que acontece se a consumidora trocar de celular?
12. Conseguimos fazer comparações longitudinais (foto antes/depois) sob cifra?
13. Onde estão os pontos de decifração inevitáveis, e como vamos justificá-los?

Custo e infraestrutura

14. Qual é o custo computacional estimado por consulta, em FHE versus plaintext?

15. Que aceleradores de hardware estamos avaliando? HEXL? FPGA? GPU específico?
16. Qual é o caminho para reduzir custo em 10× nos próximos 18 meses?
17. Vamos construir interno ou usar vendor (Zama, Duality, Inpher)?
18. Qual é o capex e o opex previstos nos próximos 24 meses?

Segurança e conformidade

19. Os parâmetros de segurança que vamos usar atendem o nível de 128 bits? Pós-quântico?
20. Quem fará a auditoria de segurança independente?
21. Como pretendemos demonstrar conformidade com LGPD art. 11 e GDPR cat. especial?
22. Conseguimos publicar a arquitetura aberta para revisão pública?
23. Qual é nosso plano de migração se um esquema for comprometido?

Produto e narrativa

24. Qual feature do produto vamos lançar primeiro com FHE?
25. Como vamos comunicar a feature à consumidora sem usar jargão?
26. Como vamos explicar para imprensa não-técnica?
27. Qual seria o claim de marketing defensável que poderíamos fazer?
28. Temos um terceiro independente disposto a validar nossas afirmações publicamente?

Riscos

29. Qual é o pior cenário se um competidor anunciar antes de nós?
30. Qual é o pior cenário se um regulador interpretar nossa arquitetura como insuficiente?

~

O Espelho que Não Vê

eBook estratégico para a alta gestão da indústria cosmética global.
Volume I · Edição 2026 · Distribuição confidencial.

Composto em Iowan Old Style e SF Pro.
Construído como documento HTML auto-contido.
Imprima em papel de gramatura alta para fidelidade ao layout original.

— fim —