

O que colar e o que não colar num chat de IA

Uma folha pra combinar com o seu time. Colar dado de cliente num chat é tratamento de dado pessoal, com regra no Brasil desde 2018. A linha existe e é mais simples do que parece.

LEIA ANTES DE USAR

Este material é educacional e **não é aconselhamento jurídico**. Ele te dá noção pra reconhecer risco e mudar hábito, não pra decidir questão jurídica da sua empresa. Caso concreto pede advogado.

O filtro que resolve a maior parte dos casos

A PERGUNTA

Se o titular do dado soubesse que você está fazendo isso, ele acharia razoável?

O cliente saber que você usou IA pra te ajudar a redigir a resposta pra ele: razoável. O cliente descobrir que a planilha inteira de clientes, com valores e histórico, foi colada num chat pra você pedir uma análise de perfil: provavelmente não.

Não cole

☐ Documento de identificação de terceiro

CPF, RG, CNH, passaporte. Se precisa extrair informação, tape os identificadores antes.

☐ Base de clientes inteira

Planilha completa, exportação do sistema, lista de contatos. O risco é desproporcional ao ganho, e quase sempre dá pra fazer a mesma análise sem os nomes.

☐ Dado sensível

Saúde, religião, política, biometria, orientação sexual. Se for inevitável no seu ramo, fale com advogado antes, não depois.

☐ Credencial

Senha, chave de acesso, token, login de sistema.

☐ **Contrato assinado inteiro, quando você só quer ajuda com uma cláusula**

Cole a cláusula, não o contrato.

Pode colar, com cuidado

☐ **Texto de cliente com o identificador removido**

"Cliente reclamou que o produto chegou com 5 dias de atraso e quer reembolso" funciona igualzinho à versão com nome, CPF e telefone. A IA não precisa saber quem é.

☐ **Dado agregado**

"Vendas de março por categoria" não identifica ninguém. É a forma mais segura de trabalhar com informação real.

☐ **Dado seu, da sua empresa**

Faturamento, processo interno, texto que você mesmo escreveu.

Três hábitos que valem mais que qualquer ferramenta

☐ **Anonimizar antes de colar**

Troque os nomes por "Cliente A", "Cliente B". Tire CPF, telefone e e-mail. Trinta segundos, e resolve a maioria esmagadora dos casos, porque o identificador quase nunca é necessário pra tarefa, ele só estava junto.

☐ **Configurar o serviço**

Confira se o conteúdo das conversas é usado pra treinar o modelo e desative se der. É uma tela de privacidade, leva dois minutos. Ferramenta muda política com frequência, reconfira de tempos em tempos.

☐ **Combinar com a equipe**

Numa empresa pequena o maior risco não é você. É quem colou a base inteira num chat gratuito porque ninguém disse que não podia. Uma regra de uma página, combinada com todo mundo, vale mais que qualquer ferramenta.

O que conta como dado pessoal

Toda informação relacionada a uma pessoa **identificada ou identificável**. A parte que surpreende é a segunda: não precisa ter o nome escrito. Se o conjunto de informações permite chegar em quem é aquela pessoa, é dado pessoal.

CATEGORIA	EXEMPLOS
Óbvios	Nome, CPF, e-mail, telefone, endereço
Menos óbvios	Número de contrato, localização, histórico de compra, gravação de voz, foto. "Cliente que comprou o imóvel da rua tal em março" identifica tão bem quanto o CPF
Sensíveis (proteção maior)	Origem racial, religião, opinião política, filiação sindical, saúde, vida sexual, biometria

Quando parar e chamar um advogado

- A IA virou parte estruturante do seu produto ou serviço.
- Você trata dado sensível de forma rotineira.
- Você pensa em treinar ou ajustar um modelo com base de dados própria.
- Aconteceu um incidente com dado pessoal, aí o relógio já está correndo.

Fontes: Lei nº 13.709/2018 (LGPD). ANPD, Nota Técnica nº 27/2024 (dados de terceiros para treinar IA generativa), Nota Técnica nº 39/2024 (caso Meta), Nota Técnica nº 1/2026 (caso Grok) e Radar Tecnológico nº 3, "Inteligência Artificial Generativa". OWASP GenAI LLM Top 10, edição 2026.