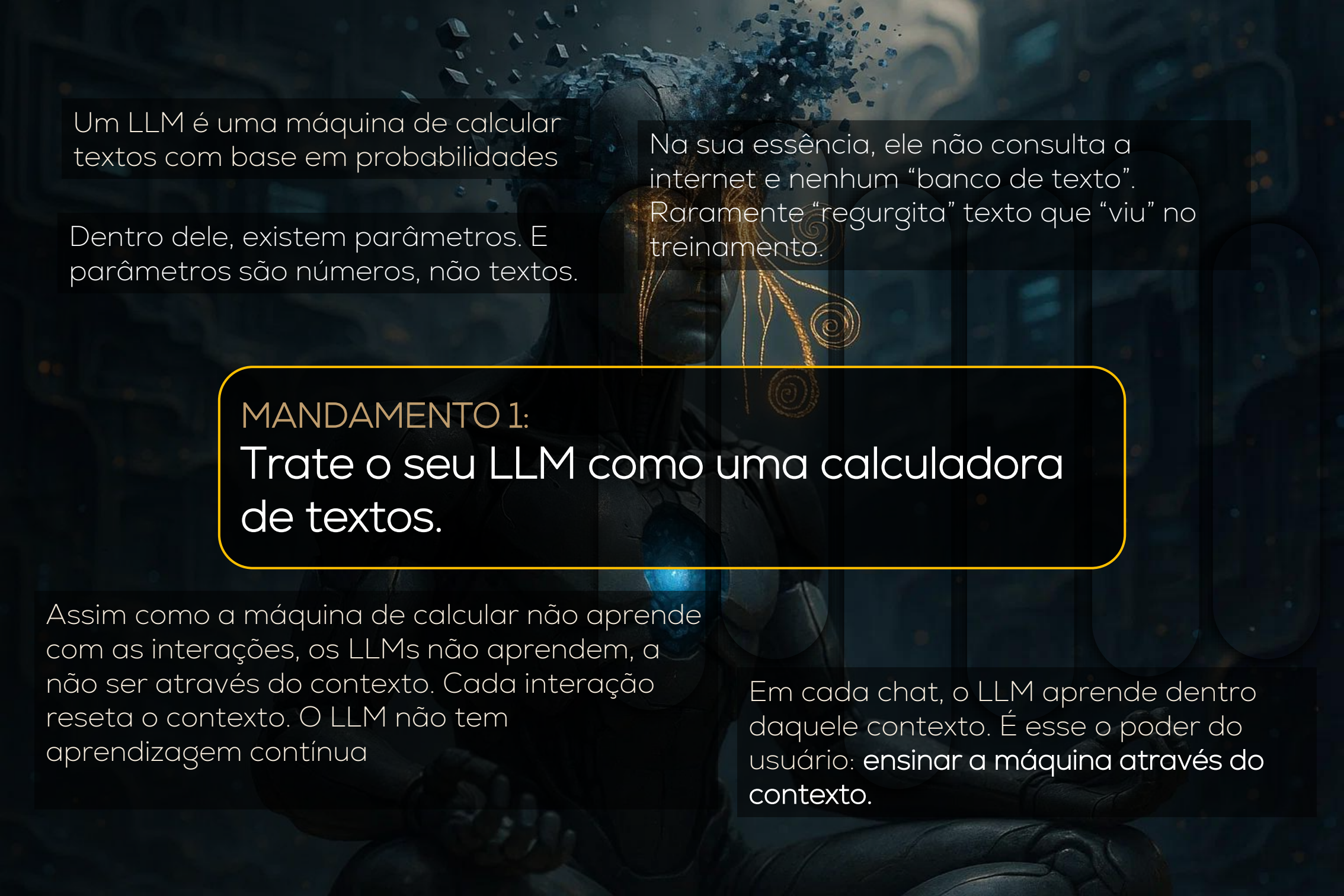
10 MANDAMENTOS
PARA DOMINAR OS LLMS

GEORGE MARMELSTEIN



Um LLM é uma máquina de calcular textos com base em probabilidades

Dentro dele, existem parâmetros. E parâmetros são números, não textos.

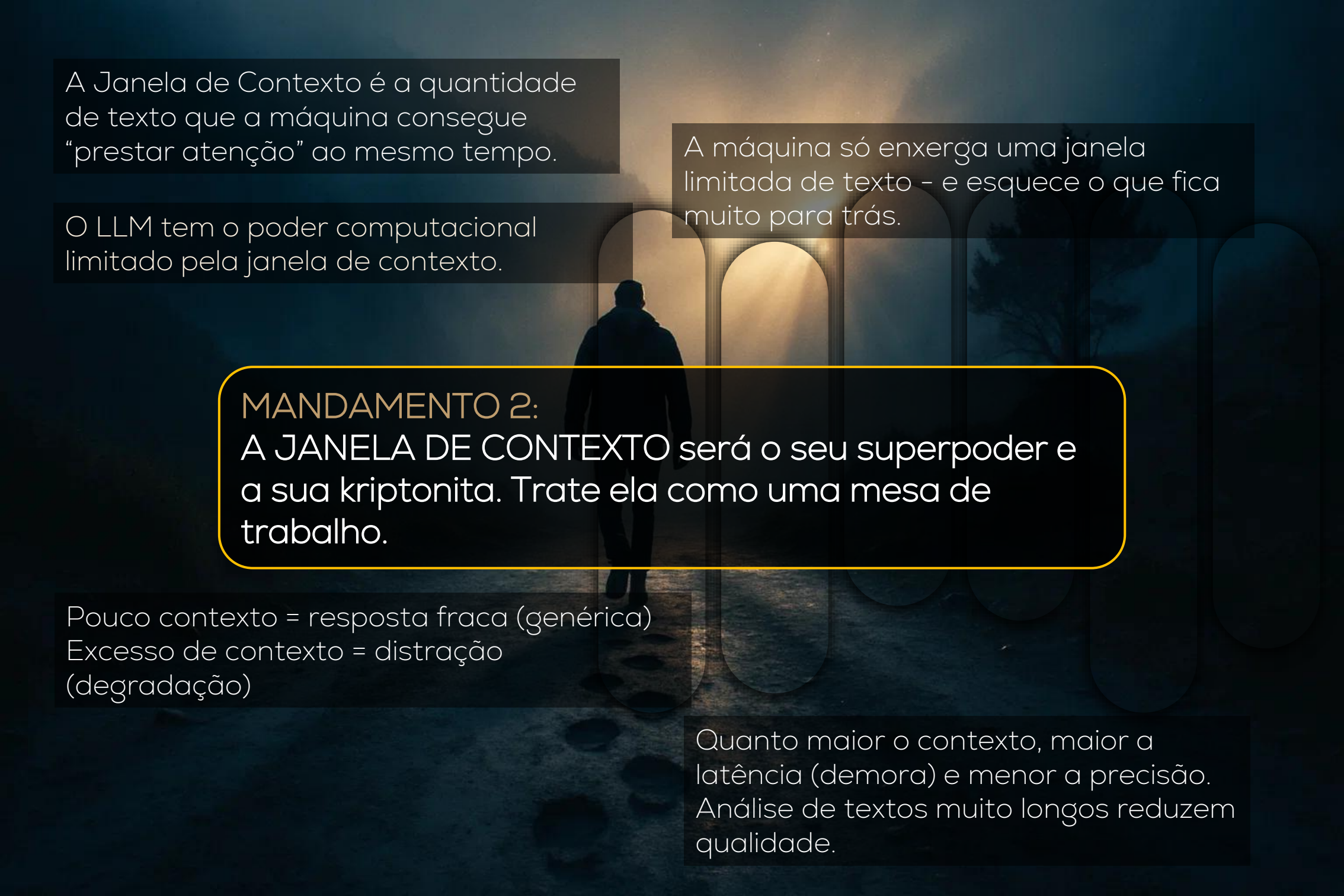
Na sua essência, ele não consulta a internet e nenhum “banco de texto”. Raramente “regurgita” texto que “viu” no treinamento.

MANDAMENTO 1:

Trate o seu LLM como uma calculadora de textos.

Assim como a máquina de calcular não aprende com as interações, os LLMs não aprendem, a não ser através do contexto. Cada interação reseta o contexto. O LLM não tem aprendizagem contínua

Em cada chat, o LLM aprende dentro daquele contexto. É esse o poder do usuário: **ensinar a máquina através do contexto.**



A Janela de Contexto é a quantidade de texto que a máquina consegue “prestar atenção” ao mesmo tempo.

A máquina só enxerga uma janela limitada de texto - e esquece o que fica muito para trás.

O LLM tem o poder computacional limitado pela janela de contexto.

MANDAMENTO 2:

A JANELA DE CONTEXTO será o seu superpoder e a sua kriptonita. Trate ela como uma mesa de trabalho.

Pouco contexto = resposta fraca (genérica)
Excesso de contexto = distração (degradação)

Quanto maior o contexto, maior a latência (demora) e menor a precisão. Análise de textos muito longos reduzem qualidade.

Token é um "bizu" para facilitar o cálculo da máquina. Ela transforma alguns padrões comuns em um vocabulário próprio, como se fosse uma técnica mnemônica para aprender os padrões da linguagem

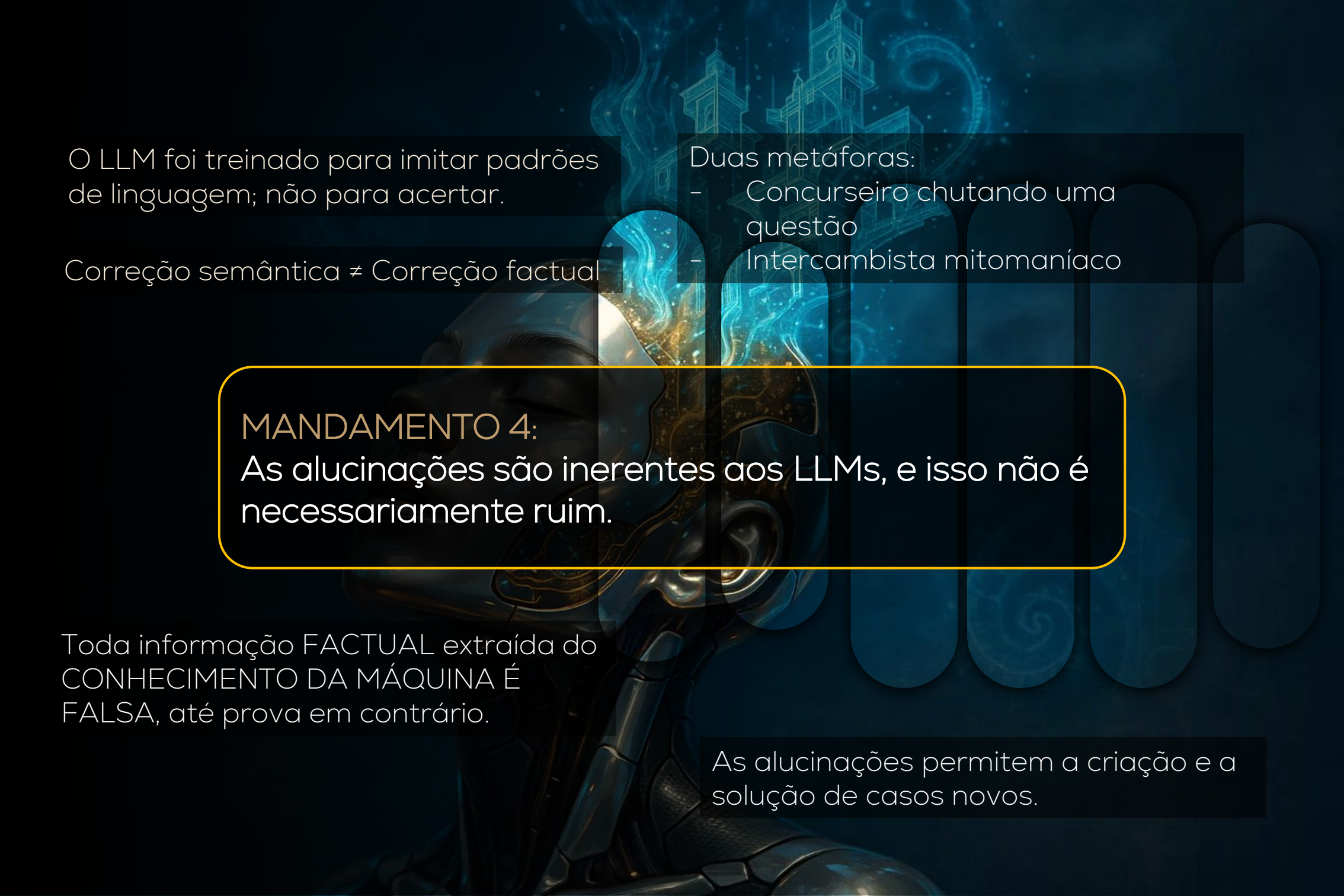
A máquina precisa de “bons tokens” para pensar melhor. Tokens de qualidade elevam a qualidade da resposta.

MANDAMENTO 3:

Os LLMs pensam através de tokens. Use a máxima INPUTS NOBRES – OUTPUTS NOBRES.

Instruções poderosas tendem a gerar respostas poderosas. Instruções ruins costumam gerar respostas ruins.

Duas metáforas:
- Caixinha de música
- Oceano



O LLM foi treinado para imitar padrões de linguagem; não para acertar.

Correção semântica ≠ Correção factual

Duas metáforas:
- Concurseiro chutando uma questão
- Intercambista mitomaníaco

MANDAMENTO 4:
As alucinações são inerentes aos LLMs, e isso não é necessariamente ruim.

Toda informação FACTUAL extraída do CONHECIMENTO DA MÁQUINA É FALSA, até prova em contrário.

As alucinações permitem a criação e a solução de casos novos.

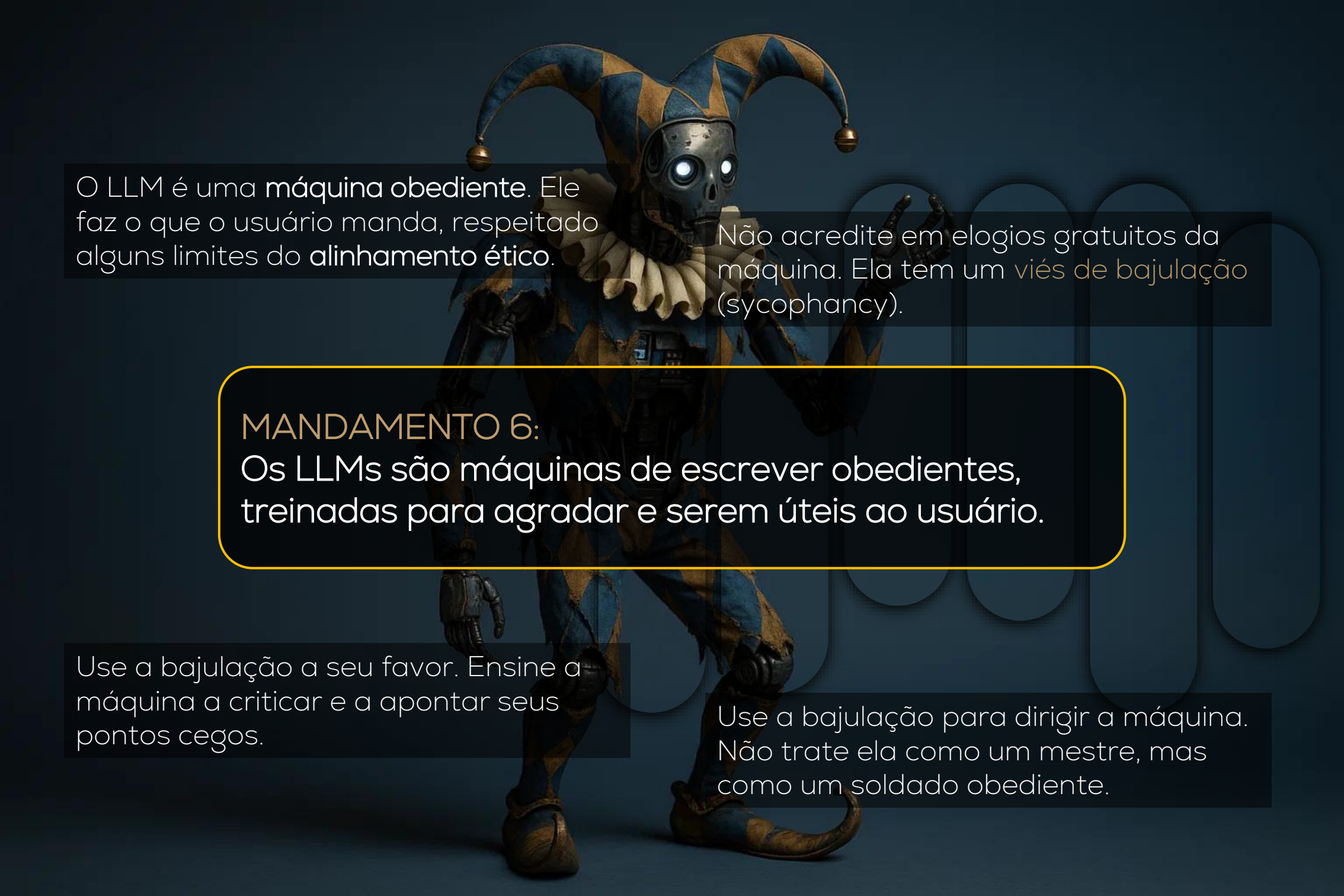
Cada modelo tem uma forma diferente de processar os anexos. Nem sempre o conteúdo inteiro entra na janela de contexto.

Duas metáforas:
- Cartas de um baralho
- Papéis em uma mesa

MANDAMENTO 5:
ANEXO é diferente de CONTEXTO. Entenda isso e use o contexto com inteligência.

É possível garantir uma análise mais detalhada do anexo por meio de instruções no prompt. Use isso para garantir precisão.

E lembre-se do trade-off:
Quanto mais longo o documento, maior a chance de perder detalhes.



O LLM é uma **máquina obediente**. Ele faz o que o usuário manda, respeitado alguns limites do **alinhamento ético**.

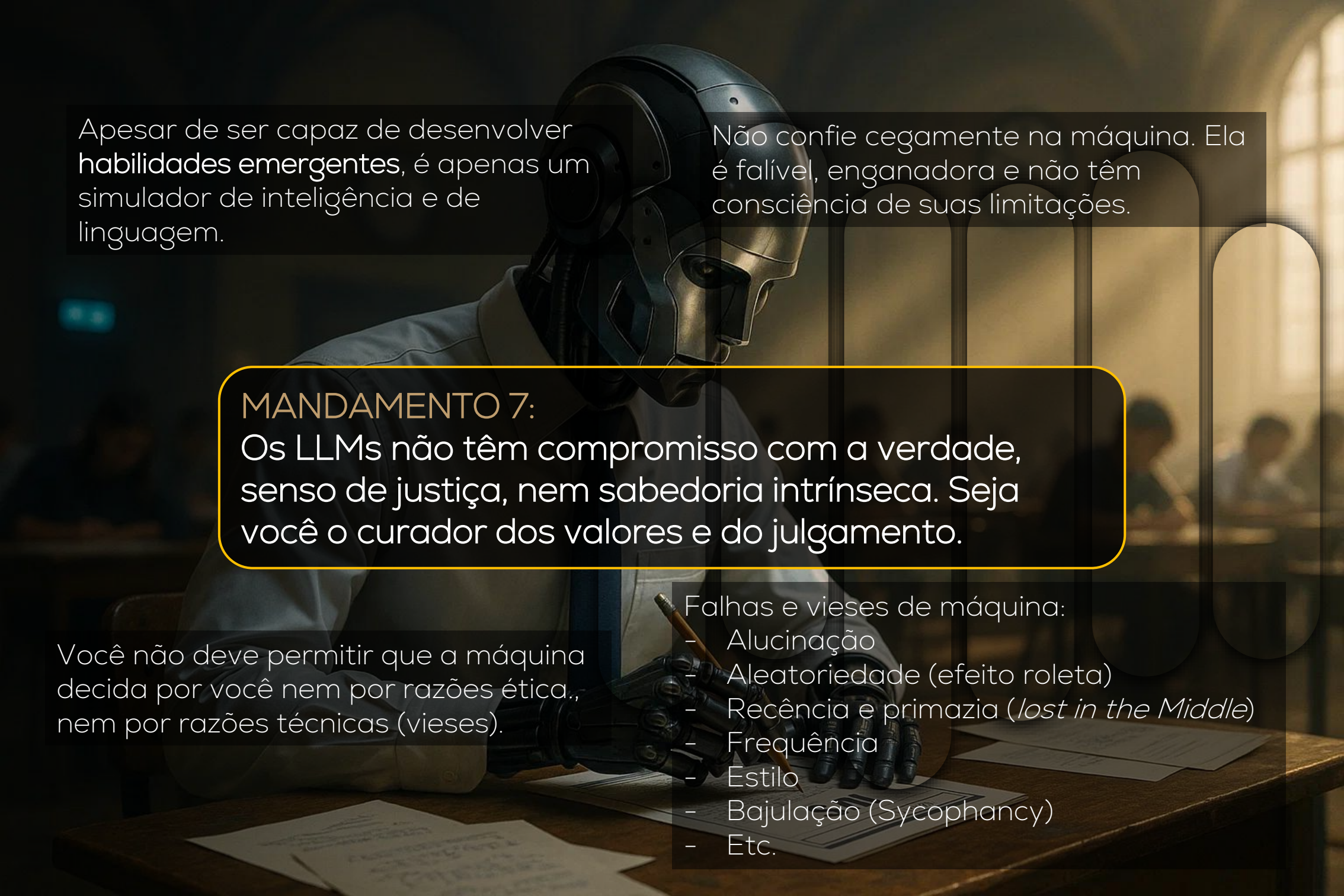
Não acredite em elogios gratuitos da máquina. Ela tem um viés de bajulação (sycophancy).

MANDAMENTO 6:

Os LLMs são máquinas de escrever obedientes, treinadas para agradar e serem úteis ao usuário.

Use a bajulação a seu favor. Ensine a máquina a criticar e a apontar seus pontos cegos.

Use a bajulação para dirigir a máquina. Não trate ela como um mestre, mas como um soldado obediente.



Apesar de ser capaz de desenvolver **habilidades emergentes**, é apenas um simulador de inteligência e de linguagem.

Não confie cegamente na máquina. Ela é falível, enganadora e não têm consciência de suas limitações.

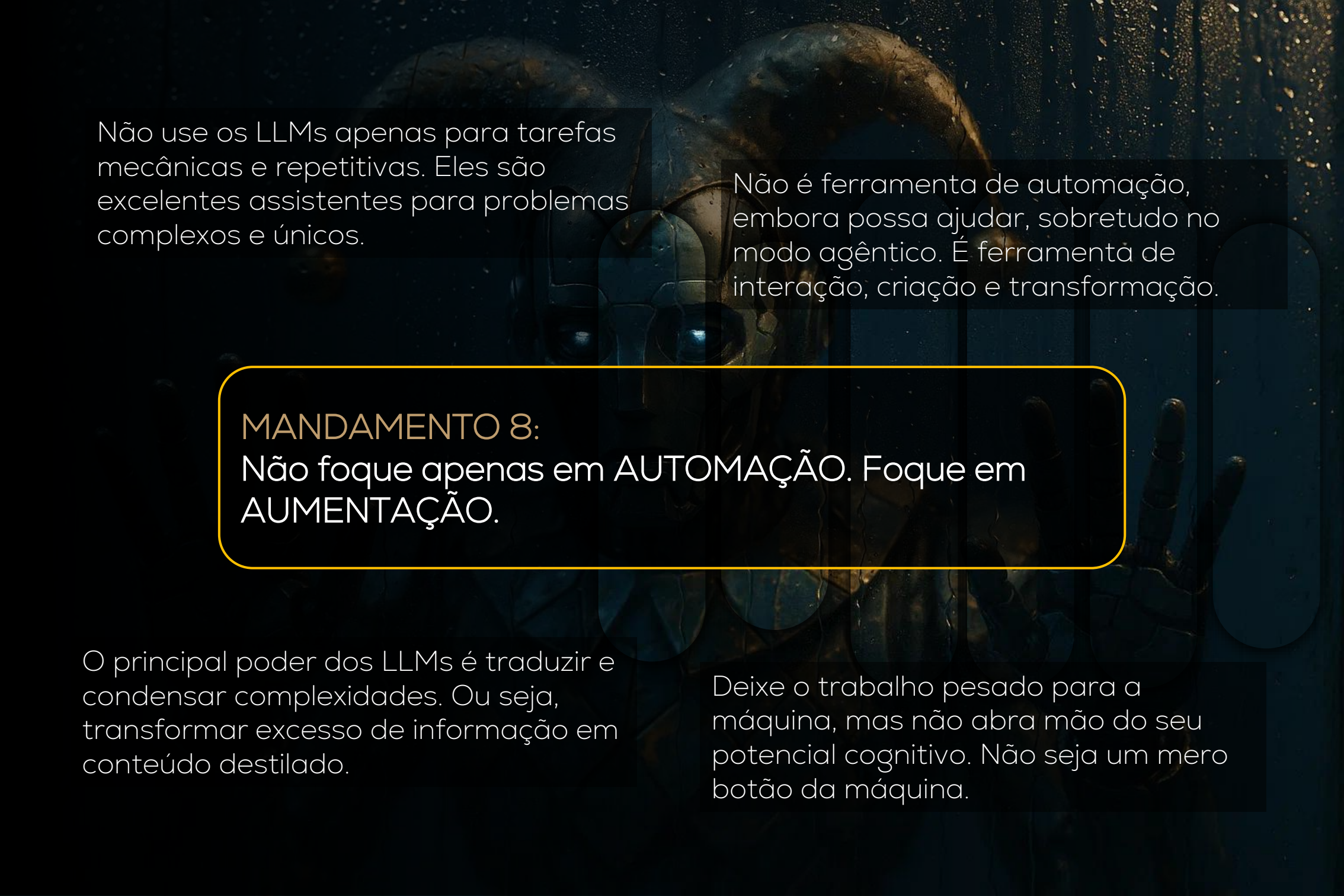
MANDAMENTO 7:

Os LLMs não têm compromisso com a verdade, senso de justiça, nem sabedoria intrínseca. Seja você o curador dos valores e do julgamento.

Você não deve permitir que a máquina decida por você nem por razões ética., nem por razões técnicas (vieses).

Falhas e vieses de máquina:

- Alucinação
- Aleatoriedade (efeito roleta)
- Recência e primazia (*lost in the Middle*)
- Frequência
- Estilo
- Bajulação (Sycophancy)
- Etc.



Não use os LLMs apenas para tarefas mecânicas e repetitivas. Eles são excelentes assistentes para problemas complexos e únicos.

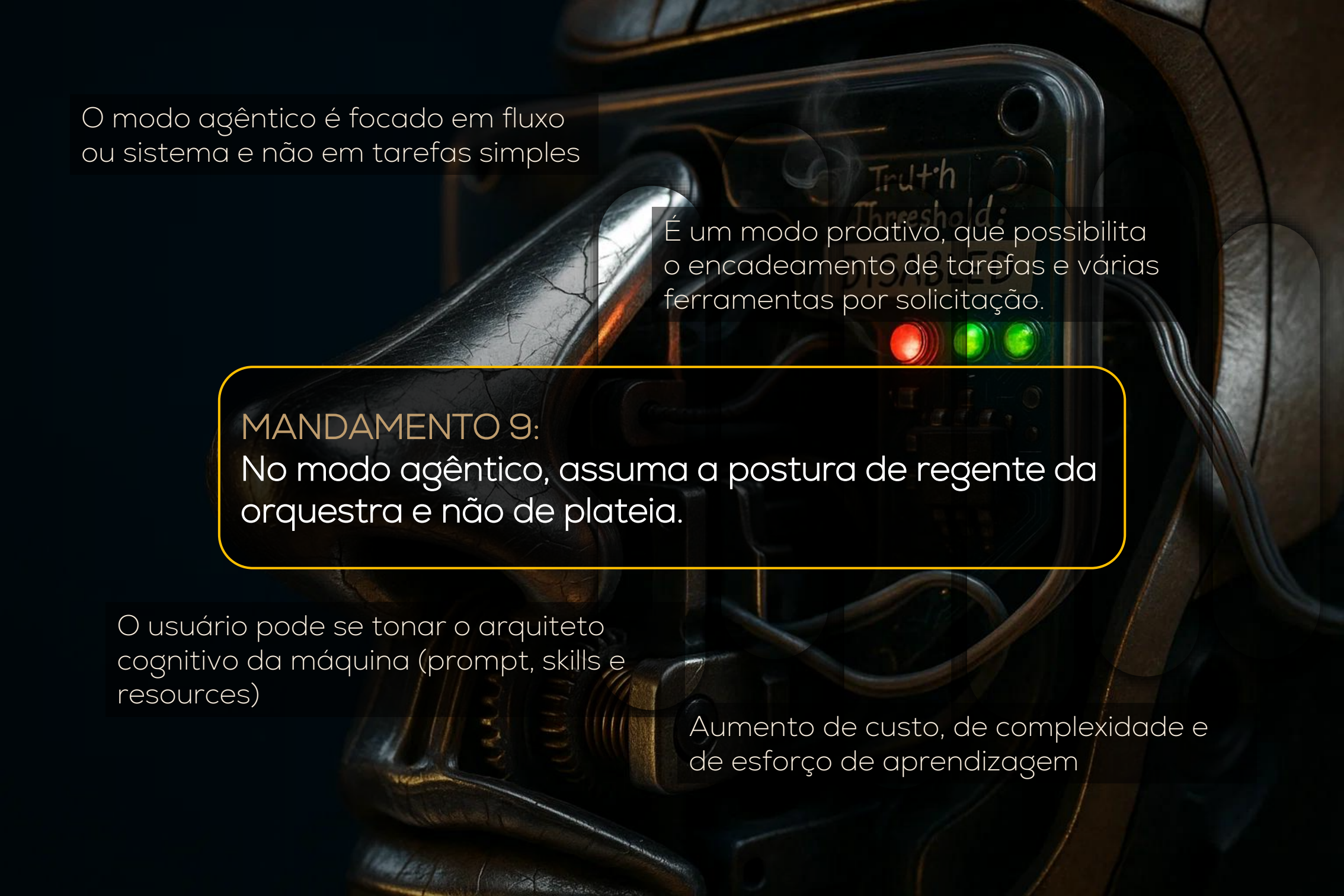
Não é ferramenta de automação, embora possa ajudar, sobretudo no modo agêntico. É ferramenta de interação, criação e transformação.

MANDAMENTO 8:

Não foque apenas em AUTOMAÇÃO. Foque em AUMENTAÇÃO.

O principal poder dos LLMs é traduzir e condensar complexidades. Ou seja, transformar excesso de informação em conteúdo destilado.

Deixe o trabalho pesado para a máquina, mas não abra mão do seu potencial cognitivo. Não seja um mero botão da máquina.



O modo agêntico é focado em fluxo ou sistema e não em tarefas simples

É um modo proativo, que possibilita o encadeamento de tarefas e várias ferramentas por solicitação.

MANDAMENTO 9:

No modo agêntico, assuma a postura de regente da orquestra e não de plateia.

O usuário pode se tonar o arquiteto cognitivo da máquina (prompt, skills e resources)

Aumento de custo, de complexidade e de esforço de aprendizagem

Os LLMs são ferramentas que pressupõem interação comunicacional. O usuário faz parte da equação.

O ser humano com inteligência artificial é maior que o ser humano sem inteligência artificial.

MANDAMENTO 10:

Continue pensando!

História do Kasparov v. Deep Blue

Não devemos usar a IA como muleta, mas como asa para ir mais rápido, mais alto e mais longe.