

REUNIÃO ORDINÁRIA · EXCLUSIVA PARA MEMBROS

COMISSÃO DE DIREITO DIGITAL E PROTEÇÃO DE DADOS · 01/09 · 19H

Prompt, Skill, HAG e Agentes: o que faz o advogado?

Ética, LGPD e a operação real de um escritório — do site à petição: extração em escala, skills, sistema e responsabilidade profissional.

Douglas Vilar · OAB/PR 47.278

Vice-Presidente da Comissão de Direito Imobiliário — Instituto Juristas · Membro Relator da Comissão de IA da OAB/PR

90 minutos ao vivo

Ética · LGPD · Skills · HAG · Agentes

Lembrete Art. 32: a IA não assina. A IA não decide sozinha. A IA não é pessoa.



DOUGLAS VILAR

ADVOGADO



Os Quatro Saltos da Advocacia: A Evolução da Infraestrutura

1. Máquina de escrever e revista do tribunal



Informação lenta, elaboração de peça levava semanas.

2. Computador e pesquisa online



Texto editável, mas com fontes de pesquisa totalmente dispersas.

3. Processo digital (PJe/Projudi)



Autos na nuvem, controle de prazo transferido para o e-mail.

4. IA generativa no fluxo do caso



A IA do advogado agora fala diretamente com a IA do juízo.

Quem trata a IA como atalho de texto, perde. Quem trata como infraestrutura — com revisão humana inegociável — escala com segurança.

O Lastro Operacional: Engenharia Jurídica em Escala Real

A operação não é teórica, é testada no mais alto rigor da prática jurídica.

+70

Skills

Automações do
escritório ativas na
operação diária.

17

Tipos

De peças cíveis
automatizadas e
validadas.

11

Automações

Focadas estritamente na
produção de conteúdo
ético.

4

Redes

Sociais operadas
diretamente por agente
de IA com revisão.

52

Julgados

Do TJPR estruturados
em uma única tese
publicada no site.

387

Processos

Na memória ativa de
aprendizado do sistema.

+16.000

Contratos

Analizados
historicamente pela
infraestrutura.

+3.000

Audiências

Realizadas na carreira,
garantindo lastro na
realidade forense.



Matriz de Ética Profissional: O Limite da Máquina

A IA não assina. O advogado assina e responde.

PERMITIDO

(Sempre com curadoria humana)

- Rascunho de peça e resumo de autos volumosos.
- Comparação de minutas e organização de fluxos.
- Pesquisa jurisprudencial assistida e revisão de linguagem.

EXIGE CAUTELA

- Inserção de dado de cliente em ferramenta de mercado.
- Citação de julgado sem conferência rigorosa da fonte original.
- Publicidade e uso de IA por estagiário sem política interna clara.

VEDADO

- Delegar a análise jurídica complexa à máquina.
- Protocolar qualquer documento sem revisão integral.
- Inventar ementa, artigo ou doutrina; quebrar o sigilo profissional.
- Inserir comando oculto na peça ou transferir independência técnica.



O Piso Normativo Existente: A Punição Já Está em Vigor

Não espere o marco legal da IA. O regramento aplicável é atual e absoluto.

- **Lei 8.906/1994 (Estatuto da Advocacia):** Art. 7º, II e Art. 34, VII determinam que o sigilo e deveres disciplinares alcançam imediatamente o dado em ferramenta externa.
- **Código de Ética e Disciplina da OAB (2015):** Arts. 25 a 27 garantem o sigilo. A curadoria do conteúdo gerado é dever intransferível do advogado, nunca da plataforma.
- **Recomendação CFOAB 001/2024:** Diretrizes nacionais para uso de IA generativa (base do Plano Nacional de IA da OAB de junho/2026).
- **TED OAB-SP (16/04/2026):** Exige supervisão humana rigorosa, revisão integral e proíbe terminantemente a confiança exclusiva no resultado.
- **Resolução CNJ 615/2025:** IA no Judiciário exige transparência e auditabilidade. É neste ambiente que o advogado protocola.
- **PL 2338/2023 (Marco Legal da IA):** Em tramitação na Câmara em 2026 (aprovado no Senado em 10/12/2024). Ainda não é lei.

Riscos Críticos e Ativos: Alucinação e Prompt Injection



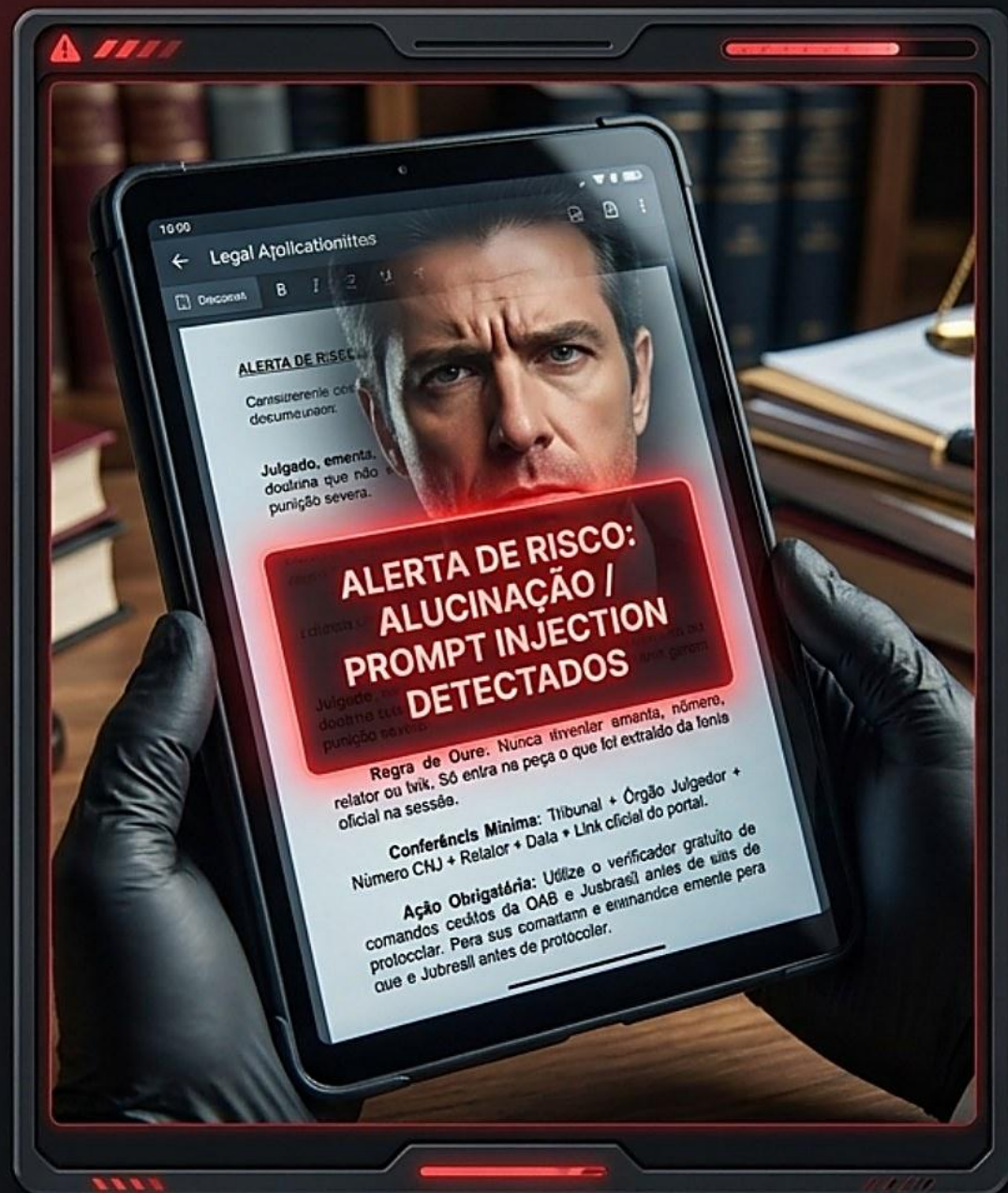
**ALUCINAÇÃO**
(Invenção de Dados)

- Julgado, ementa, artigo ou doutrina que não existem geram punição severa.
- **Regra de Ouro:** Nunca inventar ementa, número, relator ou link. Só entra na peça o que foi extraído da fonte oficial na sessão.
- **Conferência Mínima:** Tribunal + Órgão Julgador + Número CNJ + Relator + Data + Link oficial do portal.



**PROMPT INJECTION**
(Fraude Processual)

- **Comando oculto** na peça para tentar manipular a IA de leitura do juízo (ex: texto em branco).
- **Agosto/2026:** Alta de fraudes identificadas. 15 multas aplicadas, 17 comunicações diretas à OAB e suspensões cautelares em seccionais.
- **Caso Real:** Maio/2026 resultou em multa trabalhista superior a R\$ 84 mil aplicada ao infrator.
- **Ação Obrigatória:** Utilize o verificador gratuito de comandos ocultos da OAB e Jusbrasil antes de protocolar.





LGPD e Sigilo 1/3: O Mapa de Responsabilidade

Colar o caso no chat não transfere sua posição jurídica.

O Escritório é o **CONTROLADOR**

- **Art. 5º, VI, LGPD:** A quem competem as decisões referentes ao tratamento de dados pessoais. O escritório define a finalidade, o meio e o limite do uso da IA.
- **Art. 39, LGPD:** O controlador responde de forma direta pelo tratamento irregular feito pelo operador. Sem um contrato de processamento de dados adequado (DPA), o risco jurídico é integral do advogado.

A IA é, no máximo, **OPERADORA**

- **Art. 5º, VII, LGPD:** Pessoa jurídica que realiza o tratamento de dados pessoais em nome do controlador. A ferramenta age estritamente sob comando, sem autonomia legal.

LGPD e Sigilo 2/3: Bases Legais e a Malha Fina Regulatória

Bases Legais (Arts. 7º e 11, LGPD)

- A base legal usual do escritório para uso de IA é a execução do contrato de honorários e o exercício regular de direitos em processo judicial.
- **Atenção Crítica:** O tratamento de dado sensível (saúde, biometria) exige obrigatoriamente a hipótese específica do art. 11.

Transparência e Decisão (Art. 20, LGPD)

- O titular dos dados tem o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado.
- O raciocínio jurídico do escritório não pode, em hipótese alguma, operar como uma caixa-preta.

Sanções Severas (Art. 52, LGPD)

- A ANPD colocou o uso de IA como prioridade absoluta na agenda regulatória 2026-2027.
- Multa de até 2% do faturamento da pessoa jurídica, com um teto implacável de R\$ 50 milhões por infração.



LGPD e Sigilo 3/3: A Política Interna de IA do Escritório

Política de prompt é medida de segurança jurídica (Arts. 46 a 49, LGPD), não capricho da equipe de TI.

O que NUNCA entra em modelo de mercado:

- **Nome completo + CPF + endereço** em chat de IA de versão de consumidor.
- **Peça inteira** contendo **dado sensível de saúde** ou dados de criança/adolescente.
- **Segredo de justiça** exposto fora de um ambiente de nuvem privativo e controlado.
- **Login, token ou senha de acesso** a qualquer sistema judicial (PJe, e-SAJ).
- **Comando antiético**: invente precedente se não achar.
- Permitir que **os autos do cliente alimentem** o treino do modelo da IA fornecedora.

O Padrão Ouro do Escritório:

- ✓ **Ambiente fechado** com **contrato Enterprise** e **opt-out** compulsório de treino de dados.
- ✓ **Pseudonimização** obrigatória na entrada (Autor A, Réu B, supressão de CPF).
- ✓ **Base de conhecimento própria** (Sistema + Drive) como fonte exclusiva da verdade.
- ✓ **Relatório de Impacto à Proteção de Dados (RIPD)** revisado anualmente.
- ✓ **Registro de auditoria** indicando qual ferramenta gerou cada minuta.
- ✓ **Revisão humana obrigatória** registrada antes do protocolo.





A Arquitetura Real: Muito Além do Chat

Três IAs soltas não resolvem um escritório.
Apenas um sistema integrado resolve.

Camada 3 — Sistema (O Cérebro Operacional):

Cadastro de clientes, autos com busca em texto integral, anotações, prazos, financeiro. A IA lê o processo real e documentado — ela não tenta lembrar de ouvir falar.

Camada 2 — Peças (O Acervo Vivo):

17 skills cíveis ativas, trabalhistas e contratos. Cada skill possui um checklist rígido, banco de teses validado e consome modelos reais do acervo histórico do escritório.

Camada 1 — Domínio (A Inteligência Setorial):

Inteligência segmentada (cível, imobiliário, locação, trabalhista). O roteador central escolhe a skill exata baseada **estritamente no número CNJ e na área.**

Camada 0 — Identidade (A Fundação):

A voz única do escritório, papel timbrado, fontes confiáveis, caminhos mapeados no Drive e política de citação. Sem essa base, cada prompt inventaria um escritório diferente.



Superfícies de Trabalho: Especialização e Limites

Grok Chat: Pesquisa profunda, construção de tese e atualização normativa.

Proibição: Não pedir peça final sem alimentar com os autos reais.

Grok Terminal: Scripts, extração de dados e organização de pastas de julgados.

Proibição: Não pedir conclusão jurídica sem revisão integral.

Claude Chat: Redação longa, análise detalhada e confronto técnico de minutas.

Proibição: Não protocolar nenhum texto gerado sem conferir o julgado na fonte.

Claude Cwork: Fila de minutas processada em lote na máquina local.

Proibição: Não gerar peça alguma com processo incompleto ou faltando anexos.

Claude Code: Criação de skills, manutenção de identidade e instalação multi-IA.

Proibição: Rigorosamente proibido inventar precedente ou doutrina.

Sistema Douglas Vilar: Integração CNJ, guarda de autos e busca avançada.

É a ferramenta de apoio do advogado — não um oráculo que o substitui.

A Parte do Claude: Chat, Cowork e Code

As três superfícies da Anthropic no escritório — da redação à construção da operação inteira.

SUPERFÍCIE 1

Claude Chat

Redação longa, análise detalhada e **confronto técnico de minutas**. Trabalha com as instruções permanentes do escritório: voz, timbrado e vedações gravadas.

Proibição: nenhum texto protocolado sem conferir o julgado na fonte.

SUPERFÍCIE 2

Claude Cowork

A IA **dentro das pastas do caso**: lê os autos, monta cronologia, aponta contradições e processa a **fila de minutas em lote** na máquina local — sem queimar crédito de API.

Proibição: peça alguma nasce com processo incompleto.

SUPERFÍCIE 3

Claude Code

Onde a operação é **construída**: as 70+ skills, o site publicado com método, a extração das 5.323 ementas, o timbrado automatizado e a **instalação multi-IA** — a mesma skill roda em Claude, Grok e Cursor.

Proibição: rigorosamente vedado inventar precedente.

O caso real: foi o Claude que recebeu todos os processos do escritório, leu tudo, classificou o acervo por área e tipo de peça, extraiu o padrão da casa — e criou as skills. O advogado revisou o manual uma vez; o erro morreu para sempre.

GROKBOT: O Agente Local e a Operação de Retaguarda

Agente de IA com nome próprio e daemon local, operando ininterruptamente no servidor físico do escritório.

Lista de Autorizações Explícitas:

- Autorizado a agir sem solicitar permissão apenas para: varreduras de dados públicos, publicações programadas e deploys de site. Todo o resto é bloqueado ou exige prompt humano.

Segurança e Auditoria Absoluta:

- Toda ação é gravada no log de auditoria com um identificador técnico próprio (usuário de serviço).
- NUNCA opera com dados sensíveis em rede aberta. NUNCA é apontado para a pasta privada do cliente.

Rotinas Agendadas e Governança:

- 17:00 e 17:45: Varre fontes oficiais de Direito Digital, novas regulações e atualizações das IAs (Grok, ChatGPT, Claude, Gemini, NotebookLM), entregando um resumo executivo diário.
- **Lição Prática:** Dois executores automáticos no mesmo repositório exigem disciplina estrita. Conferência de produção é obrigatória antes e depois de qualquer publicação.



O Site: Tese Jurídica Publicada com Método

O site não é uma vitrine institucional passiva. É o rigor técnico da advocacia exposto ao mercado.

1. Definição: Tese rigorosa entre aspas (ex: golpe do falso advogado), criação de slug estável e pasta canônica no Drive.

2. Extração Bruta: Extração SEM IA de portais oficiais (TJPR, TJSP e-SAJ, TJSC, STJ SCON, TST) garantindo ementa, relator e link íntegros.

3. Classificação Manual: Separação primária (a favor/contra/parcial) baseada apenas no resultado final do julgado.

4. Análise Generativa: Só agora a IA atua: identifica por que a tese venceu/perdeu e cria clusters fáticos (padrões).

5. Dupla Camada: Construção da página pública com topo em linguagem acessível ao leigo, e base altamente técnica para advogados (com árvore de decisão).

6. Publicação. Artigo técnico no ar, garantindo total transparência do método de apuração utilizado.



Extração em Escala e a Prova do Método

Primeiro se extrai o dado bruto oficial; só depois se aplica a inteligência generativa.

Caso Âncora

O **Caso Âncora**: Uma única tese jurídica resultou em 52 julgados reais mapeados do TJPR. Zero ementas inventadas. Cada link aponta rigorosamente para o portal oficial do tribunal. O método replica para qualquer tese.



O que a IA **NUNCA** faz (A Fronteira Intocável)

- - Não inventa ementa de jurisprudência.
- - Não completa nome de relator por suposição.
- - Não cita decisão sem incluir o link original da fonte.
- - Não mistura regras e costumes de tribunais distintos.
- - Não analisa o mérito antes de extrair o dado completo.

O que a IA **Efetivamente FAZ** (A Escala de Valor)

- - Agrupa milhares de dados em clusters de comportamento processual.
- - Explica sistematicamente os motivos de vitória e derrota.
- - Monta uma árvore de decisão visual para casos futuros.
- - Gera o checklist fundamental da peça inicial.
- - Redige o escopo narrativo da página pública.

Petição Automática: O Fluxo Baseado no Processo

A minuta de qualidade nasce da leitura profunda dos autos, nunca de um prompt genérico solto.



1. CNJ

Identificação do processo pela numeração. Bloqueio nativo: sem autos completos, recusa-se a gerar a peça.

2. Autos

A IA lê e isola apenas o trecho crítico para o ato (sentença, planilha de cálculos ou decisão impugnada).

3. Memória

Varredura da própria base em busca da peça de maior aderência já protocolada pelo escritório.

4. Skill

Ativação da instrução estruturada exata para o tipo de peça, injetando as teses mapeadas do acervo.

5. Timbrado

Aplicação estrita do template oficial da banca. O cabeçalho corporativo permanece intocado.

6. Pasta

Salvamento automático na taxonomia correta: Cliente / Número CNJ / Data do evento.

Petição Automática: Regras Inegociáveis de Protocolo

O rigor operacional que blinda o escritório e protege o cliente.

- ✓ - **Processo Incompleto = Zero Peça:** O sistema trava *by design* se houver ausência de documentação crítica dos autos.
- ✓ - **Tolerância Zero para Invenção:** Toda menção de lei exige número, artigo, parágrafo e inciso. Todo julgado exige tribunal, órgão julgador, número CNJ, relator, data exata e link.
- ✓ - **Preservação da Identidade:** A peça deve exalar a voz institucional histórica da banca, rechaçando textos prolixos e artificiais de chatbots genéricos.
- ✓ - **Rastro Gravado:** Toda minuta gerada deixa um log inalterável no histórico do processo dentro do sistema.

O Ato Soberano (A Revisão Humana)

O advogado lê a minuta final com o mesmo rigor de quem lê um texto ditado a um assistente. A Regra Suprema: Se o advogado não assinaria aquela página específica com confiança absoluta, ele jamais protocola.





1. Entreguei os Processos: O histórico de anos do escritório (autos e peças protocoladas) foi inserido no sistema.



2. A IA Leu Tudo: Análise volumétrica de cada processo, argumento e desfecho judicial.



3. Classificou: Acervo segmentado por área (cível, imobiliário, trabalhista), tipo de peça e sucesso da tese.



4. Extraíu o Padrão: A máquina mapeou teses favoritas, cláusulas repetidas e capturou a voz da casa.



5. Criou as Skills: 387 processos na memória viraram +70 skills catalogadas (17 tipos cíveis).



6. Teste e Produção: Teste exaustivo contra caso fictício. Só entra em produção nas IAs após checklist validado em caso real.



Como Nasce Uma Skill: Da Leitura em Massa à Automação

Skill não é salvar um prompt favorito. É o protocolo do escritório encapsulado em código.

Anatomia de um SKILL.md

- ✓ **- Regra codificada de Ouro:** não inventa jurisprudência, pergunta se faltar fato e nunca assina.
- ✓ **- A Regra de Nascimento:** O fluxo se repetiu 3 vezes? Documenta-se o acerto/erro, cria-se o arquivo e instala-se na rede. Corrige-se o erro apenas uma vez — e ele morre para sempre.



Conteúdo e Captação: A Ética Inegociável da Publicidade

A autoridade jurídica não age como agência de marketing de massa. A publicidade exige rigor processual.

Limites Éticos e Normativos da OAB:

- ✓ - **CED OAB (Arts. 39 a 47):** Publicidade estritamente informativa, discreta e moderada. É terminantemente vedado o sensacionalismo, captação ilícita e qualquer promessa de resultado.
- ✓ - **Provimento CFOAB 205/2021:** Regula o meio digital, exigindo identificação expressa e proibindo o merchandising agressivo e a comparação desleal com colegas.

A Regra da Produção de Conteúdo com IA:

- ✓ - **Postar tese jurídica** gerada por IA sem conferir o julgado original é o mesmo vício ético de protocolar petição com ementa falsa. Todo post exige fonte oficial verificada.
- ✓ - **Gestão de Leads e LGPD:** O prospecto que chega pelo WhatsApp vira cadastro seguro no Sistema próprio, com triagem humana. O dado de um lead atrai a proteção total da LGPD. Nunca se opera com planilhas soltas na nuvem.

O Relógio do Escritório: A Operação de Retaguarda

A operação sistêmica baseada em agentes autônomos não espera o advogado acordar para produzir valor.

17:00 e 17:45 — O GROKBOT realiza a varredura de regulação de Direito Digital e compila o relatório.

07:30 — Publicação automatizada (aprovada na véspera) distribuída em 4 redes sociais.

12:00 e 22:00 — Coleta automática de KPIs de engajamento, tráfego e conversão.

02:00 — Varredura autônoma e fechamento de conciliação do sistema financeiro.

03:00 — Agente realiza análise de pautas, coleta jurisprudência diária e estrutura cards visuais.

03:30 — Compilação autônoma do artigo técnico longo, com formatação e fontes.

06:00 — Processamento de vídeo: extração de cortes longos de podcast para Reels.

Operação Contínua: Triagem de novos leads e registro auditável (rastro de tudo).

Segunda-feira de Manhã: Os 7 Atos de Implementação

O checklist imediato para migrar do uso amador para a operação de nível institucional.

1.

Política de Uma Página: Defina por escrito o que vai para a IA, o que é sigilo absoluto, quem revisa e quem protocola.

2.

Inventário de Ferramentas: A conta pessoal de IA de um estagiário ou sócio não é o ambiente corporativo do escritório.

3.

Caso-Piloto de Validação: Escolha um único tipo de peça, num único tribunal, com dez autos reais. Meça o ganho de tempo e a taxa de erro.

4.

A Fonte Oficial: Estabeleça a regra de ouro: toda ementa sai virgem do portal do tribunal. A IA atua apenas para agrupar depois.

5.

Padronização de Pastas: Instaure imediatamente o salvamento rígido: Arquivo -> Cliente / Número CNJ / Data.

6.

O Checklist de Protocolo: Implante a etapa final: Julgado conferido? Dado revisado? Comando oculto checado? O líder de fato leu tudo?

7.

A Primeira Skill: Isole o fluxo que o escritório já repetiu mecanicamente três vezes e documente para criar a automação fundacional.





Perguntas Frequentes: O Pragmatismo da IA na Advocacia

Q: Preciso saber programar código?

A: Não. O que o advogado precisa saber com urgência primária é identificar e recusar peremptoriamente uma ementa inventada.

Q: Posso colar a íntegra de um processo no ChatGPT?

A: Somente em ambiente com contrato corporativo (Enterprise), base legal definida (LGPD) e dados pseudonimizados. A conta pessoal não é ambiente seguro.

Q: E se o magistrado usar IA na elaboração da decisão?

A: O Judiciário é regulado pela Resolução CNJ 615/2025. Tentar inserir comando oculto na peça para burlar a leitura do juiz é fraude processual, não inovação.

Q: A Inteligência Artificial substitui a figura do estagiário?

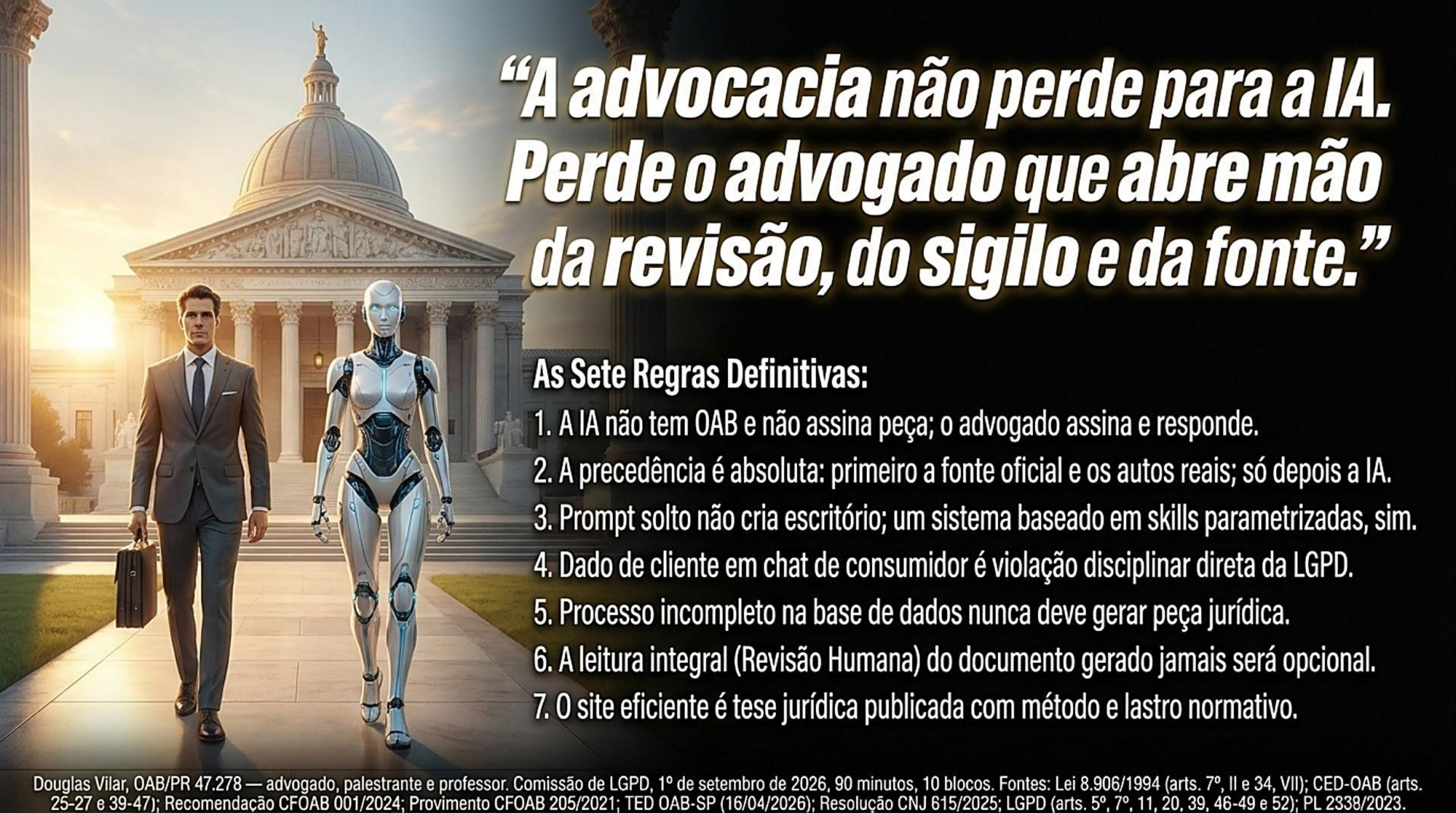
A: A IA substitui o retrabalho operacional e burocrático. Ela jamais substitui a necessidade da leitura atenta dos autos, nem a responsabilidade civil técnica.

Q: Por onde devo começar a implementação amanhã?

A: Por uma política documentada de uma página, escolhendo um único tipo de peça, isolando dez processos, focando na fonte oficial.

Q: Como deve operar o marketing utilizando automação por IA?

A: Como operação de autoridade técnica pura, sob a estrita égide do CED-OAB (arts. 39-47) e do Provimento CFOAB 205/2021.

A man in a dark suit and tie walks alongside a silver humanoid robot. They are walking on a paved path towards a large, classical building with a prominent dome and columns, reminiscent of a government or judicial building. The scene is set during sunset or sunrise, with warm light illuminating the scene from the left.

***“A advocacia não perde para a IA.
Perde o advogado que abre mão
da revisão, do sigilo e da fonte.”***

As Sete Regras Definitivas:

1. A IA não tem OAB e não assina peça; o advogado assina e responde.
2. A precedência é absoluta: primeiro a fonte oficial e os autos reais; só depois a IA.
3. Prompt solto não cria escritório; um sistema baseado em skills parametrizadas, sim.
4. Dado de cliente em chat de consumidor é violação disciplinar direta da LGPD.
5. Processo incompleto na base de dados nunca deve gerar peça jurídica.
6. A leitura integral (Revisão Humana) do documento gerado jamais será opcional.
7. O site eficiente é tese jurídica publicada com método e lastro normativo.