Dossie Lantyer - Como Avaliar Ferramentas Juridicas de I

Uma metodologia prática para juristas avaliarem IA jurídica com foco em LGPD, sigilo, alucinação, fornecedores, segurança, governança e responsabilidade profissional.

Resumo executivo

A fase da curiosidade acabou. A inteligência artificial já está sendo usada por juristas para organizar ideias, resumir documentos, revisar textos, sugerir estruturas de parecer, apoiar pesquisa jurídica, comparar argumentos, revisar contratos e acelerar rotinas. O problema central não é mais perguntar se a IA pode ser útil. Pode. A pergunta madura é outra: em quais condições ela pode ser usada sem expor dados, violar sigilo, fabricar autoridade jurídica, fragilizar a responsabilidade profissional ou criar dependência tecnológica invisível?

Ferramenta jurídica de IA não deve ser avaliada como aplicativo comum. O Direito depende de fonte, data, jurisdição, autoridade, contexto, ônus argumentativo e responsabilidade profissional. Uma resposta fluente pode estar errada. Uma citação pode existir e ainda assim não sustentar a conclusão. Uma base jurídica pode estar desatualizada. Um prompt pode conter dado pessoal, estratégia processual ou segredo profissional. Um fornecedor pode prometer segurança no marketing e limitar quase toda responsabilidade no contrato.

Este dossiê propõe a Matriz Lantyer de Avaliação de IA Jurídica, com critérios para uso, contratação e recomendação de ferramentas de IA em ambientes jurídicos. A matriz combina Direito Digital, LGPD, ética profissional, segurança da informação, avaliação de modelos, procurement jurídico e governança institucional.

A ideia é simples: IA jurídica pode aumentar capacidade de trabalho, mas só vira ferramenta profissional quando entra em uma arquitetura de governança.

Tese central

Qual IA é adequada para esta tarefa, com estes dados, este risco, esta supervisão, esta governança e esta responsabilidade?

Nove erros comuns

01 - Comprar pela promessa de produtividade

A promessa típica é simples: "economize horas de trabalho". A pergunta melhor é: economiza horas depois da revisão?

Se a ferramenta gera resposta em 30 segundos, mas exige duas horas de conferência porque mistura fontes, omite exceções ou responde com excesso de segurança, talvez não haja produtividade líquida. Há apenas deslocamento do esforço: menos redação, mais auditoria.

02 - Confundir fluência com confiabilidade

Modelos de linguagem são bons em produzir texto plausível. Isso é útil, mas perigoso. O texto pode soar técnico, elegante e assertivo mesmo quando contém erro. No Direito, a forma da resposta não prova a correção da resposta.

Fluência não é fundamento. Elegância não é fonte.

03 - Ignorar dados e confidencialidade

O risco começa antes da resposta. Começa no prompt. Um contrato copiado, uma petição anexada, uma planilha de clientes, um histórico médico, um documento trabalhista ou uma estratégia processual podem carregar dados pessoais, dados sensíveis, sigilo profissional e informação estratégica.

Se a ferramenta não é adequada para receber esse dado, o problema já aconteceu antes mesmo de a IA responder.

04 - Achar que "revisão humana" resolve tudo

Supervisão humana pode ser séria ou simbólica. Revisão séria confere fontes, testa premissas, verifica exceções, compara com documentos originais, mede risco e assume responsabilidade. Revisão simbólica é apenas clicar, aprovar ou ler por cima.

Human-in-the-loop não é humano no carimbo. É humano no controle.

05 - Não testar com casos reais anonimizados

Demo comercial é teatro controlado. Teste institucional precisa usar amostras próprias, anonimizadas quando possível, com tarefas reais, critérios claros e registro de erros.

A ferramenta que impressiona na apresentação pode falhar no cotidiano do escritório.

06 - Não pedir documentação do fornecedor

Não basta perguntar "é seguro?". Pergunta vaga gera resposta vaga. O correto é pedir DPA, política de retenção, lista de suboperadores, documentação de segurança, logs, política de treinamento, localização dos dados, SLA, plano de incidente e cláusulas de responsabilidade.

07 - Não definir usos proibidos

Toda política séria precisa dizer o que não pode ser feito. Sem zona vermelha, a equipe decide no improviso. E improviso com dado de cliente é roleta russa com vocabulário corporativo.

08 - Não criar política interna

Sem política, cada pessoa decide sozinha o que pode entrar no prompt, qual ferramenta usar e o que precisa de revisão. O resultado é previsível: critérios divergentes, dados expostos por boa-fé e nenhum registro do que foi feito. Política interna não é burocracia; é a diferença entre uso governado e sorte acumulada.

09 - Proibir tudo e criar Shadow AI

A proibição absoluta parece segura, mas pode empurrar a equipe para ferramentas pessoais, contas gratuitas, celulares próprios e uso escondido. A organização perde visibilidade e controle. O risco deixa de existir no papel e passa a existir no subterrâneo.

Matriz Lantyer - 30 criterios

Bloco A: Finalidade, tarefa e dados nucleares

- 1. Finalidade de uso: Para que exatamente a ferramenta será usada? | Evidencia: Documento de casos de uso e limites declarados. | Risco: Médio
- 2. Tipo de tarefa jurídica: A tarefa envolve pesquisa, minuta, contrato, prova, atendimento, gestão ou decisão? | Evidencia: Matriz de funcionalidades por tarefa. | Risco: Alto
- 3. Tipo de dado inserido: Que dado será enviado à ferramenta? | Evidencia: Política de classificação de dados. | Risco: Alto
- 4. Dados pessoais: Há informação sobre pessoa identificada ou identificável? | Evidencia: Mapeamento de tratamento e base legal. | Risco: Alto
- 5. Dados sensíveis: Há saúde, biometria, origem racial, convicção, vida sexual, dado genético ou similar? | Evidencia: RIPD quando pertinente, controles adicionais. | Risco: Alto
- 6. Sigilo profissional: O conteúdo envolve relação advogado-cliente? | Evidencia: Cláusula de confidencialidade, não treinamento, segregação. | Risco: Alto

Bloco B: Confidencialidade estendida e cadeia de tratamento

- 7. Segredo de justiça: O documento está sob restrição judicial? | Evidencia: Política de uso proibido/condicionado. | Risco: Alto
- 8. Informação estratégica: Há tese, negociação, segredo empresarial ou risco reputacional? | Evidencia: Classificação de confidencialidade. | Risco: Alto

- 9. Retenção de dados: Por quanto tempo prompts, arquivos e outputs são armazenados? | Evidencia: Política de retenção e deleção. | Risco: Alto
- 10. Uso para treinamento: O fornecedor usa dados do usuário para treinar, ajustar ou avaliar modelos? | Evidencia: Cláusula expressa de não treinamento ou opt-out. | Risco: Alto
- 11. Transferência internacional: Dados saem do Brasil? Para onde? | Evidencia: Mapa de dados e cláusulas de transferência. | Risco: Alto
- 12. Suboperadores: Quais terceiros tratam dados no serviço? | Evidencia: Lista de suboperadores e direito de notificação. | Risco: Alto

Bloco C: Segurança, acesso e auditoria

- 13. Controle de acesso: Quem pode acessar a ferramenta e os dados? | Evidencia: RBAC, MFA, SSO, perfis e permissões. | Risco: Médio/Alto
- 14. Logs e auditoria: Há registro de uso, prompts, arquivos e respostas? | Evidencia: Exportação de logs e trilha de auditoria. | Risco: Alto
- 15. Segurança da informação: Como a ferramenta previne vazamento, manipulação e acesso indevido? | Evidencia: Relatórios de segurança, pentest, controles OWASP. | Risco: Alto
- 16. Certificações e evidências: O fornecedor tem certificações ou auditorias relevantes? | Evidencia: ISO 27001, SOC 2, ISO/IEC 42001, quando aplicáveis. | Risco: Médio

Bloco D: Qualidade jurídica, fontes e supervisão

- 17. Validação de fontes: A resposta mostra fontes verificáveis e contextualizadas? | Evidencia: Demonstração com fontes, links, trechos e datas. | Risco: Alto
- 18. Atualização da base jurídica: A base está atualizada? Com qual frequência? | Evidencia: Log de atualização e escopo de cobertura. | Risco: Alto
- 19. Risco de alucinação: Que tipos de erro a ferramenta comete? | Evidencia: Benchmark independente, testes locais, relatório de falhas. | Risco: Alto
- 20. Capacidade de recusa: A ferramenta sabe dizer que não sabe? | Evidencia: Testes com perguntas sem base ou com lacunas. | Risco: Médio/Alto
- 21. Explicabilidade mínima: A ferramenta explica o caminho da resposta? | Evidencia: Documentação de método e justificativa. | Risco: Médio
- 22. Supervisão humana: Quem revisa, quando e como? | Evidencia: Protocolo de revisão por nível de risco. | Risco: Alto

Bloco E: Contrato, governança e implementação

- 23. Responsabilidade por erro: Quem responde por falha, vazamento ou indisponibilidade? | Evidencia: Termos, SLA, indenização, limitação de responsabilidade. | Risco: Alto
- 24. Integração com fluxo de trabalho: A IA acessa e-mail, drive, GED, CRM ou processo? | Evidencia: Mapa de integrações e escopos de permissão. | Risco: Alto
- 25. Vendor lock-in: É possível exportar dados e migrar? | Evidencia: Plano de saída e formato de exportação. | Risco: Médio
- 26. Custo total: Qual é o custo real além da licença? | Evidencia: TCO, proposta detalhada e custos variáveis. | Risco: Médio
- 27. Ordenamento brasileiro: A ferramenta foi testada no Direito brasileiro? | Evidencia: Testes com legislação e jurisprudência brasileiras. | Risco: Alto
- 28. Testes locais: A instituição testou com casos próprios anonimizados? | Evidencia: Relatório de piloto, critérios e pontuação. | Risco: Alto
- 29. Política interna: O uso está coberto por política clara? | Evidencia: Política de uso, semáforo e treinamento. | Risco: Alto
- 30. Plano de incidente: O que acontece se houver vazamento, erro ou citação falsa? | Evidencia: Playbook de incidente e responsáveis. | Risco: Alto

Semaforo de uso

Verde: uso geralmente permitido

Exemplos: brainstorming genérico, organização de ideias, revisão linguística de texto sem dados reais, explicação conceitual, roteiro de aula, estrutura inicial de artigo, checklist abstrato.

Condicao minima: sem dado de cliente, sem informação confidencial, sem citação jurídica usada sem conferência.

Quem aprova: o próprio usuário, se a política interna permitir.

Amarelo: uso condicionado

Exemplos: resumo de documento anonimizado, estrutura de parecer, comparação de argumentos, minuta inicial de contrato simples, apoio em pesquisa preliminar, preparação de reunião.

Condicao minima: anonimização adequada, revisão humana, conferência de fontes, ferramenta autorizada quando houver documento real.

Quem aprova: responsável pela equipe ou profissional sênior.

Vermelho: uso proibido em ferramenta aberta ou sem contrato adequado

Exemplos: dados de cliente identificável, dados sensíveis, segredo de justiça, estratégia processual, documentos trabalhistas sensíveis, prova, relatório final para cliente, peça processual com jurisprudência, análise de chance de êxito.

Condicao minima: ferramenta institucional autorizada, contrato robusto, política interna, revisão humana substantiva, logs e validação de fontes.

Quem aprova: jurídico sênior, DPO, segurança ou comitê interno, conforme o caso.

Roxo/preto: uso proibido salvo autorização formal e ambiente controlado

Exemplos: bases de clientes, documentos sob segredo de justiça, grandes volumes de dados pessoais, dados de crianças e adolescentes, dados de saúde, material probatório, automação decisória, integração com sistemas internos sensíveis.

Condicao minima: autorização formal, ambiente controlado, DPA, análise de risco, segurança, logs, plano de incidente e revisão qualificada.

Quem aprova: alta gestão, jurídico, DPO, segurança e, no setor público, autoridade competente e controles internos quando aplicável.

Checklists por perfil

Advogado autônomo

- O conteúdo tem dado de cliente?
- Tem dado sensível?
- Tem estratégia processual?
- Tem documento confidencial?
- A ferramenta é aberta ou contratada com garantias?
- O fornecedor usa meus prompts para treinamento?
- Há retenção dos dados?
- A resposta tem fonte verificável?
- Eu conferi lei, jurisprudência e números?
- Eu conseguiria explicar ao cliente como usei a ferramenta?
- Eu assinaria esse resultado como meu?

Regra pratica: se você não sabe o que acontece com o dado, não coloque dado de cliente.

Escritório de advocacia

- Faça inventário das ferramentas já usadas.
- Crie política interna simples e aplicável.
- Separe usos verdes, amarelos, vermelhos e roxo/preto.
- Proíba dados de cliente em ferramenta aberta.
- Defina protocolo de conferência de fontes.
- Estabeleça quem revisa documentos finais.
- Treine sócios, associados, estagiários e administrativo.
- Inclua regras para timesheet, honorários e transparência.
- Exija DPA, não treinamento, retenção limitada e logs de fornecedores.
- Crie canal para dúvidas e incidentes.

Regra pratica: política que só proíbe cria Shadow AI; política que orienta traz o uso para a governança.

Departamento jurídico

- Envolva jurídico, DPO, segurança, compras, TI e área usuária.
- Avalie dados empresariais estratégicos, não só dados pessoais.
- Verifique suboperadores e transferência internacional.
- Exija plano de incidente e notificação.
- Avalie integração com sistemas internos.
- Teste com casos anonimizados.
- Exija portabilidade e plano de saída.
- Inclua cláusulas sobre treinamento, retenção e confidencialidade.
- Meça produtividade líquida após revisão.
- Documente a decisão de aprovação ou rejeição.

Regra pratica: se a ferramenta entra no fluxo corporativo, ela entra no mapa de risco corporativo.

Procuradorias e setor público

- Distinguir apoio administrativo, apoio redacional, análise jurídica e decisão.
- Verificar base normativa e política institucional.
- Classificar dados de cidadãos, servidores e processos.
- Evitar ferramenta aberta com dados reais.
- Exigir logs, transparência e prestação de contas.
- Garantir revisão humana efetiva.
- Avaliar impacto em direitos fundamentais.
- Considerar controles internos e auditoria.
- Cuidar de procurement público e motivação administrativa.
- Não automatizar decisão sem governança específica.

Regra pratica: no setor público, a régua é mais alta porque o risco não é apenas privado; é institucional e democrático.

Professores e pesquisadores

- Explique que IA não substitui fonte primária.
- Proíba bibliografia inventada.
- Exija declaração de uso quando a instituição assim determinar.
- Diferencie apoio de escrita, apoio de pesquisa e autoria.

- Ensine verificação de fontes.
- Não aceite citação que o aluno não leu.
- Teste ferramentas em temas de Direito brasileiro.
- Oriente sobre dados pessoais em pesquisa.
- Use IA como objeto de crítica, não como oráculo.
- Preserve integridade acadêmica.

Regra pratica: IA pode ajudar a pensar, mas não deve terceirizar autoria, leitura ou responsabilidade intelectual.

Protocolo de validacao de fontes

1. Verifique se a fonte existe.
2. Leia o trecho relevante na fonte primária ou base confiável.
3. Confira se a fonte está vigente ou atualizada.
4. Confira se a jurisdição é adequada.
5. Verifique se há entendimento contrário relevante.
6. Analise se o precedente é aplicável ao caso concreto.
7. Registre a conferência quando o risco for alto.
8. Remova qualquer citação não verificada.

Plano de 30 dias

Semana 1 - Diagnóstico e inventário

Objetivo: descobrir o que já está em uso e onde estão os riscos.

- mapear ferramentas usadas;
- identificar contas pessoais e extensões;
- levantar tarefas com IA;
- classificar dados tratados;
- identificar áreas de maior risco.

Entregaveis: inventário inicial, mapa de riscos e lista de usos urgentes a bloquear.

Go/no-go: há uso sensível em ferramenta aberta? Se sim, interromper e orientar imediatamente.

Semana 2 - Política e classificação de dados

Objetivo: criar regras mínimas.

- aprovar semáforo de uso;
- definir dados proibidos;
- criar política interna mínima;
- estabelecer responsáveis;
- criar canal de dúvidas.

Entregaveis: política v1, semáforo e guia rápido para equipe.

Go/no-go: a equipe entende o que pode e não pode fazer?

Semana 3 - Testes e fornecedores

Objetivo: avaliar ferramenta autorizada ou candidata.

- enviar perguntas ao fornecedor;

- solicitar DPA, política de retenção, suboperadores e segurança;
- rodar teste local;
- pontuar outputs;
- analisar contrato.

Entregaveis: relatório de piloto, matriz de pontuação e parecer de risco.

Go/no-go: os riscos críticos foram respondidos com evidência?

Semana 4 - Treinamento, piloto e auditoria

Objetivo: iniciar uso controlado.

- treinar equipe;
- iniciar piloto com casos de baixo/médio risco;
- registrar incidentes e dúvidas;
- ajustar política;
- definir revisão periódica.

Entregaveis: treinamento concluído, piloto ativo, plano de auditoria e backlog de melhorias.

Go/no-go: a ferramenta pode expandir para novos usos ou deve permanecer limitada?

FAQ essencial

Advogado pode usar ChatGPT no trabalho?

Pode usar IA generativa como apoio, desde que preserve sigilo, confidencialidade, proteção de dados, competência profissional e revisão humana. O risco aumenta quando há dados de cliente, documento confidencial, fonte jurídica não conferida ou uso em documento final.

Posso colocar dados de cliente em IA?

Em ferramenta aberta ou sem contrato adequado, a resposta prudente é não. Em ferramenta institucional, depende da finalidade, base legal, DPA, retenção, treinamento, segurança, suboperadores, transferência internacional e política interna.

Ferramenta paga é necessariamente segura?

Não. Ferramenta paga pode oferecer controles melhores, mas segurança depende de contrato, arquitetura, retenção, não treinamento, logs, suboperadores, certificações, plano de incidente e adequação ao uso.

IA jurídica pode inventar jurisprudência?

Sim. Pode inventar fonte, distorcer fonte real, usar precedente inaplicável ou ignorar atualização. Por isso, toda fonte jurídica deve ser conferida em base confiável antes de uso profissional.

O que é alucinação jurídica?

É erro produzido pela IA que cria ou distorce autoridade jurídica: citação inexistente, lei revogada, precedente mal aplicado, tese sem base, erro de jurisdição ou resposta plausível sem fundamento verificável.

O que é RAG e por que importa?

RAG é técnica que combina busca em documentos com geração de resposta. Importa porque pode ancorar a resposta em fontes. Mas não elimina erro: se a busca recupera documentos ruins ou incompletos, a resposta também pode falhar.

O que perguntar antes de contratar uma legaltech de IA?

Pergunte sobre dados, treinamento, retenção, suboperadores, transferência internacional, logs,

segurança, base jurídica, atualização, fontes, SLA, responsabilidade, auditoria, portabilidade e incidentes.

Escritório precisa de política interna de IA?

Sim, se o uso for profissional ou recorrente. A política reduz improviso, protege dados, orienta equipe, cria critérios de revisão e diminui Shadow AI.

O que é Shadow AI?

É o uso informal ou clandestino de IA fora da política institucional. Acontece quando pessoas usam contas pessoais, ferramentas gratuitas ou extensões sem autorização, contrato ou governança.

O que significa supervisão humana real?

Significa revisão substantiva: conferir fontes, checar fatos, avaliar aplicabilidade, corrigir erros, considerar exceções e assumir responsabilidade pelo documento final.

IA pode revisar contratos?

Pode apoiar revisão, identificar cláusulas, organizar riscos e sugerir pontos de atenção. Mas contratos sensíveis exigem análise humana, contexto negocial, confidencialidade e revisão jurídica final.

IA pode fazer pesquisa jurisprudencial?

Pode apoiar pesquisa preliminar, mas não deve substituir validação em fonte primária ou base confiável. Pesquisa jurisprudencial exige conferência de existência, atualidade, contexto e aplicabilidade.

Posso usar IA em caso com segredo de justiça?

Somente com ambiente controlado, autorização institucional, contrato adequado, segurança, logs e política específica. Em ferramenta aberta, não. E, em matéria de prova, o alerta é maior: o STJ já excluiu relatório produzido com IA generativa por falta de confiabilidade epistêmica mínima (HC 1.059.475/SP).

O cliente precisa ser informado?

Depende do tipo de uso, do contrato, dos dados envolvidos, do impacto no serviço e de diretrizes aplicáveis. Se houver processamento de dados do cliente por terceiro, impacto relevante ou exigência contratual, a transparência deve ser analisada expressamente.

Como testar uma ferramenta antes de contratar?

Use casos de uso reais, amostras anonimizadas, tarefas padronizadas, critérios de pontuação, conferência humana, análise de segurança e revisão contratual. Não aceite apenas a demo do fornecedor.

Nota editorial

Este dossiê tem finalidade educacional, editorial e estratégica. Ele não substitui parecer jurídico, auditoria de segurança, avaliação de impacto à proteção de dados, due diligence contratual ou análise individual de ferramenta.

Nenhuma ferramenta específica é recomendada neste material. A adoção de IA em ambiente jurídico depende do contexto, dos dados tratados, da finalidade, do contrato, da arquitetura técnica, das obrigações profissionais, da política institucional e do risco tolerado.

O objetivo do Dossiê Lantyer é oferecer uma régua inicial: clara o suficiente para orientar decisões e rigorosa o suficiente para evitar encantamento tecnológico.