

Beyond Algorithms – Why Responsible AI Matters

Indian LegalTech Network x August



Case Study

The employment team at Lawfirm X was faced with a detailed review of contracts for nearly 20,000 employees at company Y for a possible merger.

This totalled almost 200,000 employment contracts which needed to be analysed and categorised within a very tight deadline for a due diligence exercise.

The goal was to understand the relative risks associated with the employment contracts to allow the company to be acquired at its most competitive price.

Usually, the firm relies on sampling around 10% of the document set which, due to the associated risks, lowered the valuation of the company. The leadership wants to change this approach.

But reviewing of the entire data room would require significant resources which will be cost-prohibitive for the client.

A new LegalTech partner proposed an AI-powered contract analysis platform that could categorise all contracts for risk in a fraction of time and cost.

What are the risks and ethical concerns in this situation?

Game-Changing Capabilities



LLMs now match or exceed human lawyer accuracy

in contract review



99.97% cost reduction

over traditional legal methods



Seconds vs. hours

to complete complex legal analysis

The Reality Check



High hallucination rates

across legal tasks



Bias varies by model

and case popularity/geography



Performance inconsistency

between demonstration and real-world application



Over reliance

deferring judgement to AI



Data security and confidentiality

exposure of sensitive data



'Black box'

makes it difficult to justify decisions and outputs



Lack of Accessibility

to legal tools across users with different resources



Unclear Accountability

between user, deployer, model



Responsible AI

- Responsible AI is an approach to developing and deploying AI that is trustworthy, ethical, and designed with power dynamics in mind while minimizing risk (The Responsible AI Institute)
- Responsible AI is critical today given the rapid advancement of AI technologies and the rise of AI use, especially in critical industries like legal.
- Responsible AI should be rooted in confidence building, rather than risk mitigation. It is an enabler, not a blocker.
- Responsible AI tools provide increasingly effective ways to inspect, understand, and govern AI models throughout their lifecycle - developer, deployer, adopter, and user.

AI Governance Frameworks

EU AI Act | NIST AI Risk Management Framework | ISO/IEC Standards on AI (e.g., ISO/IEC 42001)

Human Approach to AI (UNESCO)



Proportionality and do no harm



Safety and security



Right to privacy and data protection



Multistakeholder and adaptive governance & collaboration



Responsibility and accountability



Transparency and explainability



Human oversight and determination



Sustainability



Awareness and literacy



Fairness and non-discrimination

Responsible AI: Development



Human-Centered Design

AI should be developed to serve a real human need, protect rights, and align with social values, rather than prioritizing efficiency alone.



Transparency

Document design choices, data sources, and limitations clearly so stakeholders understand how and why the system works as it does.



Fairness

Identify, test for, and mitigate bias in training data and outputs to prevent discriminatory impacts.



Accountability

Assign clear responsibility for decisions and outcomes of AI systems, ensuring developers and deployers remain answerable.



Safety & Robustness

Stress-test models to ensure they perform reliably under different conditions and cannot be easily manipulated.



Privacy by Design

Minimize data collection, protect sensitive information, and embed privacy safeguards into the system architecture from the start.

Responsible AI: Adoption and Use



Governance & Oversight

Have an AI lead, committee or just a designated team member to oversee Responsible AI in practice.



Risk Assessment Methodology

Create a risk measurement process that works for you, accounting for tool risk, use case risk and outcome risks.



Policies & Guardrails

Approve tools, define allowed use cases, and require human review where risks are higher.



Awareness & Training

Train your team in the basics of AI safety to embed Responsible AI into culture.



Adoption Practices

Explain what each tool is for, why it's being used, and make sure it fits into workflows.



Monitoring & Audit

Regularly review how tools are used, whether risks have shifted, and update policies as needed.



Compliance & Transparency

Ensure use complies with legal obligations and be open with clients and third-parties when AI is in play.



Incident Response

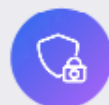
Have a clear plan for what to do if the tool fails, misuses occur, or outputs cause harm.

Responsible AI: Procurement



Transparency & Explainability

Questions to Ask: What model powers your tool - is it proprietary or third-party? How does your system generate classifications, summaries, or outputs?



Data Security & Confidentiality

Questions to ask: Where is client data stored and processed? Is our data segregated from other customers' data? Do you use client inputs for model training or fine-tuning? What security certifications do you hold?



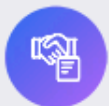
Bias & Fairness

Questions to ask: How do you test for and mitigate bias in your system?



Reliability & Performance

Questions to ask: How do you measure and report accuracy, hallucination rates, or error rates? Is there ongoing monitoring and reporting?



Accountability & Governance

Questions to ask: Who is accountable if outputs are inaccurate or harmful? Do you provide indemnities or liability coverage, and do you allow external audits or governance reviews of your system?



Lifecycle & Sustainability

Questions to ask: How do you communicate model or feature updates to clients?



So what does all this mean in practice?