DIGITAL MEDIA & ELECTRONIC COMMUNICATIONS

Think before you prompt: How employee use of AI can shape your organisation’s legal position before lawyers become involved

20 August 2026 *9 min read*

by Tebogo Sibidla, Director

The legal lifecycle begins long before a dispute reaches court, or a regulator commences an investigation. It starts when employees negotiate contracts, evaluate acquisitions, respond to regulators, investigate complaints, interpret legislation and make commercial decisions with legal consequences. Increasingly, employees turn to generative artificial intelligence (“AI”) before consulting legal advisers. They routinely ask AI to review contracts, interpret legal requirements, summarise documents and recommend courses of action. As a result, AI is becoming part of the organisation’s legal decision-making process. By the time a lawyer becomes involved, AI may already have influenced the commercial decisions taken, the information presented, and the organisation’s legal position itself.

Many organisations have developed AI governance frameworks addressing cybersecurity, privacy, intellectual property, acceptable use and regulatory compliance. However, comparatively little attention has been given to how employee use of AI can affect an organisation’s legal position. By the time a matter reaches the legal department, AI may have already influenced multiple stages of the legal lifecycle. Employees may have –

- asked AI whether contracts may be terminated, whether regulatory approval is required, whether a contractual provision is enforceable, whether an employee may be dismissed or how best to respond to a regulator;
- uploaded confidential contracts, board papers or correspondence to public AI platforms;
- asked AI to prepare a briefing for internal or external legal advisers;
- asked AI whether the organisation has a legal defence;
- generated summaries of evidence or lengthy document sets;
- prepared investigation reports using AI;
- drafted witness statements with AI assistance; or
- asked AI to recommend a litigation or regulatory strategy.

Each of these interactions has the potential to affect the organisation’s legal position in ways that may not become apparent until much later.

The risk is not simply that AI may produce inaccurate answers. Employees may unknowingly allow AI to influence how legal issues are framed, what information is presented to legal advisers, and which decisions are taken before legal advice is obtained.

This issue is no longer theoretical. Recent judicial decisions demonstrate that courts are applying long-established legal principles—confidentiality, legal professional privilege, evidential integrity and professional accountability—to the use of AI.

The question for boards, executives and General Counsel is no longer whether employees are using AI—in many organisations, everyday business practice has already answered that. The more important question is whether organisations are governing that use before it influences contracts, transactions, regulatory engagement, investigations and the legal advice upon which significant business decisions depend.

AI is increasingly influencing legal advice before legal advisers become involved

Generative AI is increasingly becoming the first point of reference when legal or regulatory questions arise—not simply a way to obtain information more quickly.

Historically, employees confronted with unfamiliar contractual provisions, regulatory obligations or employment issues would seek guidance from legal teams before taking significant decisions. Today, many employees first consult AI. This behavioural shift has important implications.

Legal advice is only as reliable as the factual information upon which it is based. If employees rely on AI to interpret contracts, summarise correspondence, identify legal issues or assess regulatory obligations before lawyers become involved, AI may shape not only the decisions taken, but also the information presented to legal advisers.

AI systems may simplify complex legal questions, present tentative propositions with unwarranted confidence, overlook jurisdiction-specific requirements or fail to appreciate commercial context. They may identify certain risks while overlooking others, prioritise commercially attractive options over legally prudent ones, or incorrectly assume that legal principles from one jurisdiction apply elsewhere.

This does not mean AI is unreliable. Sound legal advice depends not only on legal rules, but also on judgment, context, and an appreciation of the organisation’s commercial objectives and risk appetite.

The objective should not be to prohibit employee use of AI, which is embedded in everyday business practice. Rather, it is to identify matters where AI may appropriately support productivity, where legal review should remain mandatory, and where public AI platforms should not be used at all.

AI can unintentionally alter an organisation’s legal position

The legal implications extend beyond the quality of legal advice received. The way employees interact with AI may itself unintentionally alter the organisation’s legal position.

Consider a transaction team negotiating a high-value acquisition. An employee uploads a draft share purchase agreement into a publicly available AI platform and asks whether the indemnity provisions are market standard. A regulatory affairs manager uploads correspondence received from a sector regulator and asks AI to prepare a proposed response. An internal investigator uploads witness statements and requests AI to identify inconsistencies before interviews are conducted.

These scenarios illustrate two significant governance risks. First, confidential commercial information may be disclosed to third-party AI providers, and organisations may have limited visibility over how uploaded information is stored, processed or used. Second, the use of public AI platforms may affect claims of confidentiality or legal professional privilege.

In *United States v Heppner*, a US federal court held that communications with publicly available AI platforms are not protected by attorney-client privilege, even where used to prepare a defence strategy or legal arguments in anticipation of litigation. Similarly, in *Secretary of State for the Home Department v Hamid*, the English High Court held that uploading client letters and Home Office decision letters to an open-source AI tool places that information in the public domain.

These decisions illustrate a broader lesson: public AI platforms should not be regarded as confidential. Organisations should distinguish between enterprise AI environments with appropriate contractual safeguards and publicly available systems whose treatment of uploaded information may differ significantly.

The governance challenge is broader than preventing inaccurate outputs. It is ensuring that employee use of AI does not reshape the organisation’s legal position through disclosure of confidential information or erosion of privilege before legal oversight occurs.

Today’s AI interactions may become tomorrow’s legal record

Many employees regard AI interactions as informal working notes or preliminary research. However, in litigation, regulatory investigations, competition inquiries, tax audits or shareholder disputes, these interactions may form part of the organisation’s legal record.

Employees frequently ask AI to summarise witness interviews, prepare chronologies, analyse documentary evidence or draft investigation reports. Those outputs may create additional records capable of scrutiny in subsequent proceedings and may become embedded in board papers, regulatory submissions, internal memoranda or legal instructions. Organisations may ultimately be required to explain not only the decisions taken, but also the role AI played in reaching them.

Discovery obligations extend beyond final documents to drafts, communications and other electronically stored information. Organisations should proceed on the basis that prompts, uploaded documents and AI-generated outputs relating to significant matters may one day require disclosure.

Recent litigation illustrates that this is no longer merely theoretical. In *Fortis Advisors LLC v Krafton Inc.*, AI communications became part of the evidence in the case. In *Goodwin v Goodwin*, the English High Court approached witness evidence with caution where draft witness statements had been uploaded to ChatGPT before being finalised. The case illustrates that AI-assisted drafting may affect the weight a court is prepared to attach to evidence where there are concerns that the statements no longer reflect the witness’s own words. In *Conservation Law Found., Inc. v. Shell Oil Co* (United States District Court, District of Connecticut Ruling of U.S. Magistrate Judge Thomas Farrish (May 2026), the court ordered the production of AI prompts used by an expert in preparing their report.

Regulators increasingly expect organisations to explain how significant decisions were reached, particularly where those decisions affect consumers, employees or regulated activities. If AI has materially influenced regulatory submissions, internal investigations or compliance assessments, organisations may be required to explain the role AI played.

AI governance should therefore extend beyond acceptable-use policies to encompass document retention, records management and investigation protocols. Organisations should preserve original source documents, avoid relying exclusively on AI-generated summaries in significant matters and ensure legal advisers have access to primary evidence. In an era where AI interactions may become part of the legal record, preserving the integrity of that record is as important as preserving the underlying documents.

The governance lessons emerging from recent cases

Recent judicial decisions do not suggest that organisations should avoid AI. Rather, they demonstrate that long-established legal principles continue to apply irrespective of the technology used.

Courts have reinforced that responsibility for the accuracy of legal work remains with the human user, not the technology. AI may assist decision-making, but it does not replace professional judgment or diminish human accountability. (See, for example, South African decision: *Mavundla v MEC: Department of Co-operative Government and Traditional Affairs, KwaZulu-Natal and Others*; US decision: *Mata v Avianca Inc.*; UK decision: *R (Ayinde) v London Borough of Haringey; Al-Haroun v Qatar National Bank*)

South Africa recently experienced these challenges. The withdrawal of the 2026 Draft National AI Policy following reports of alleged fictitious AI-generated references reminds us that AI-assisted work remains subject to human accountability, whether in the public or private sector.

Conclusion

AI can influence your organisation’s entire legal lifecycle—from negotiating contracts and pursuing acquisitions to responding to regulators, conducting investigations, managing compliance and resolving disputes.

Much discussion surrounding AI has focused on responsible use of AI by lawyers. That debate remains important, but overlooks an equally significant challenge: AI is influencing legal issues long before lawyers become involved. It may shape the information presented to legal advisers, alter an organisation’s legal position and create records subject to regulatory or judicial scrutiny.

Organisations should therefore move beyond generic AI governance and adopt a **legal lifecycle governance** approach that identifies where AI may appropriately support legal and commercial decision-making, where legal oversight should remain mandatory, and where public AI platforms should not be used.

The organisations that derive the greatest value from AI are unlikely to be those that adopt AI the fastest. They will be those that recognise AI is changing how legal risk emerges within organisations. Where legal risk may be influenced long before lawyers are consulted, effective AI governance is about governing the legal consequences of how the technology is used.

Tebogo Sibidla

Director

View Profile