JUTA
POPIA PORTAL

ISSUE NO 71 • POPIA AND AI: FRIENDS, FRENEMIES OR FUTURE PARTNERS? • JULY 2026

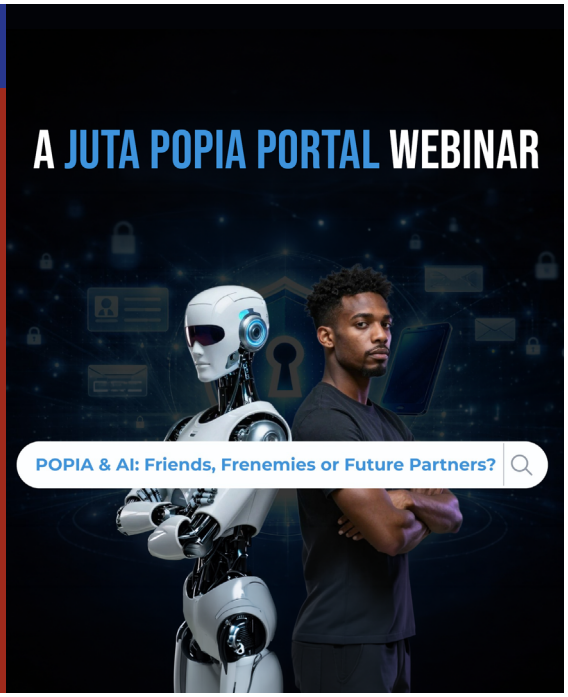
POPIA AND AI: FRIENDS, FRENEMIES OR FUTURE PARTNERS?

1. OVERVIEW

Artificial intelligence is no longer experimental. It is already embedded in ordinary business activities, from drafting documents and profiling customers to automating decisions, monitoring behaviour, generating content and analysing risk.

At Juta's May 2026 webinar, **POPIA and AI: Friends, Frenemies or Future Partners?**, Advocate Pansy Tlakula, Chairperson of the Information Regulator, placed AI firmly in the POPIA context. Her message was practical: AI may offer efficiency and competitiveness, but it must still comply with existing law. POPIA should remain the legal backbone of AI regulation in South Africa, with AI-specific rules complementing rather than replacing it.

The central takeaway is that POPIA and AI are not enemies, but they are not automatic partners either. They become workable partners only when AI governance is built around POPIA's core disciplines: privacy protection, minimality, data quality, transparency, accountability, explainability, security safeguards and fair automated decision-making.



2. AI HAS MOVED FROM NOVELTY TO NECESSITY

Photo: iStock

Advocate Tlakula noted that AI initially raised concerns about privacy, professional autonomy and oversharing on digital platforms. Regulators face a familiar problem: technology moves first and regulation follows. But AI has now shifted from novelty to operational necessity, which makes compliance more important, not less.

Daniel Solove, one of the leading scholars in privacy law, makes a similar point. Many AI privacy problems are not entirely new; AI often 'remixes' existing privacy risks in more complex and powerful ways. It can intensify concerns about data collection, inference, decision-making, surveillance, identification and accountability. For POPIA purposes, that matters because AI is not outside the privacy framework. It depends on data, and often on personal information.

Photo: iStock

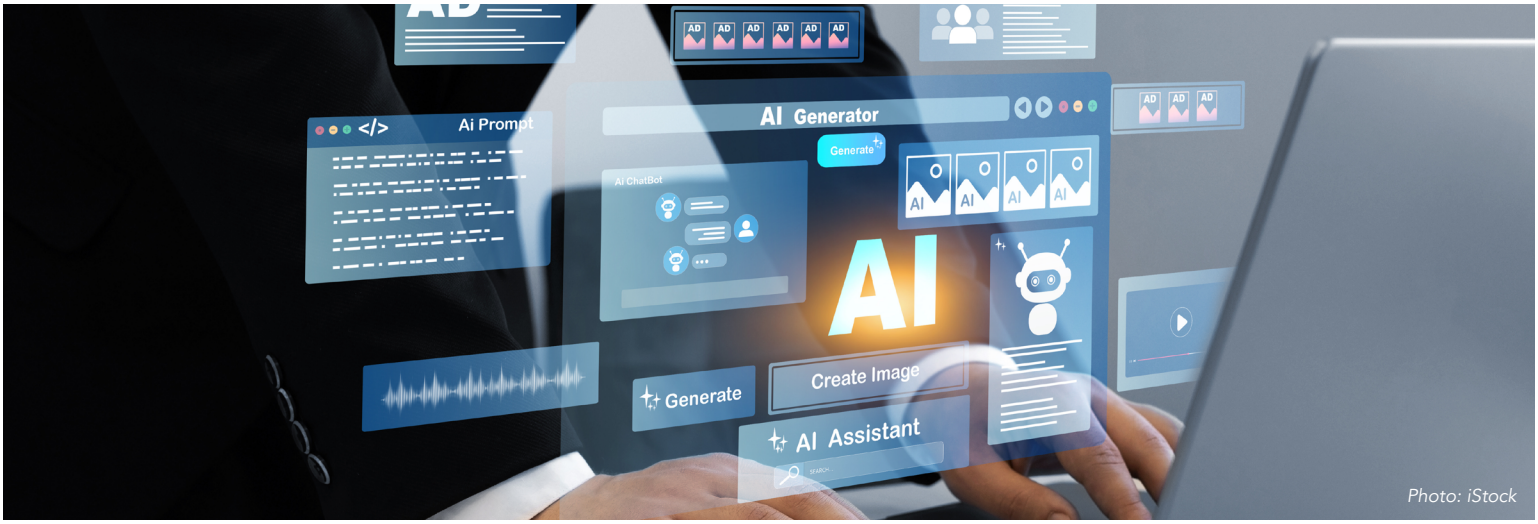


Photo: iStock

3. WHY POPIA AND AI ARE FRENEMIES

The growing reliance on AI is precisely why its tension with POPIA matters. Advocate Tlakula described POPIA and AI as 'frenemies' because AI systems often rely on large-scale data collection, profiling and automated decision-making. Those features can sit uneasily with POPIA's requirements around minimality, purpose limitation, consent, openness and accountability.

The tension becomes clear in practice:

- AI systems often need large datasets, while POPIA requires personal information to be adequate, relevant and not excessive.
- AI systems generate new patterns and inferences, while POPIA requires clear and lawful purposes.
- AI systems can be opaque, while POPIA requires openness and accountability.
- AI systems may make or influence decisions about people, while section 71 regulates certain decisions based solely on automated processing.

Advocate Tlakula identified the main risks as excessive collection, profiling, continuous monitoring, the use of special personal information, poor data quality, discriminatory outcomes, opaque decision-making, facial recognition, predictive analysis, behavioural tracking and weak security safeguards.

The real question is not simply whether we can use AI, but whether we can explain, justify, secure and control it.

4. THE WITHDRAWN AI POLICY IS A GOVERNANCE LESSON


Photo: iStock

This governance gap becomes even clearer when AI is used to produce policy or regulatory material itself. The webinar referred to South Africa's withdrawn draft national AI policy, which Advocate Tlakula used as an example of AI risk because the document reportedly included hallucinated authorities.

AI outputs can look authoritative while being wrong. That means organisations using AI for legal, compliance, policy or governance work need clear controls for source checking, human review, version control, record-keeping and accountability. The organisation should be able to identify who remains responsible for the final output and what evidence is retained to support it.

5. PRIVACY BY DESIGN MUST START EARLY


Photo: iStock

Advocate Tlakula criticised the tendency to mention POPIA only in general terms in new laws or policies without truly embedding privacy by design. In the AI context, privacy cannot be bolted on after the tool has already been procured or deployed.

The EDPB-commissioned report on privacy risks and mitigations in large language models reaches the same conclusion. Privacy risks arise across the full AI life cycle: data collection, pre-processing, training, validation, deployment, monitoring, updates and retirement.

A practical AI privacy assessment should ask questions such as:

- What personal information is used in training, fine-tuning, prompts, retrieval, logs or monitoring?
- Is special personal information involved?
- Is the data source lawful and appropriate?
- Is the purpose clear and proportionate?
- Are outputs checked for accuracy, bias and unfairness?
- Can data subjects exercise their rights?
- Are security safeguards adequate?
- Is there meaningful human oversight where decisions affect people?

6. DATA QUALITY, EXPLAINABILITY AND ACCOUNTABILITY MATTER


Photo: iStock

Advocate Tlakula emphasised data quality as a central AI concern. If an AI system relies on inaccurate, incomplete or outdated data, it may produce unfair or discriminatory outcomes. That is not merely a technical problem; it can quickly become a POPIA problem.

The same is true of explainability. Many AI systems are difficult to interpret, which weakens accountability in practice. The EDPB has also warned that AI models trained on personal data cannot automatically be treated as anonymous. That assessment must be made case by case, especially where personal data may be extracted from, inferred from, or obtained through interaction with a model.

Responsible parties should therefore avoid assuming that POPIA stops applying once data has been 'put into a model'.

7. CONCLUSION: THE PARTNERSHIP DEPENDS ON GOVERNANCE


Photo: iStock

POPIA and AI can become future partners, but not by accident. AI's appetite for data pushes directly against POPIA's disciplines of minimality, purpose limitation, openness, quality, accountability and security.

Advocate Tlakula's message was cautious but constructive: AI should not be rejected simply because it is risky, but it must be governed. POPIA should remain the backbone of that governance in South Africa.

The key questions remain straightforward:

- Where did the data come from?
- Why are we using it?
- Is the use proportionate?
- Can we explain it?
- Can we secure it?
- Can we prove it?

In South Africa, responsible AI use will depend not only on innovation, but on the discipline to govern data lawfully, transparently and responsibly.

8. READ MORE


Photo: iStock

- Chapter 15: Profiling, automated decision-making and 1984
- European Commission: European approach to artificial intelligence – AI Act
- Stanford University Human-Centered Artificial Intelligence: Rethinking Privacy in the AI Era
- 'Artificial Intelligence and Privacy' by Daniel J Solove
- AI Privacy Risks & Mitigations in Large Language Models by Isabel Barbera
- European Data Protection Board Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

juta