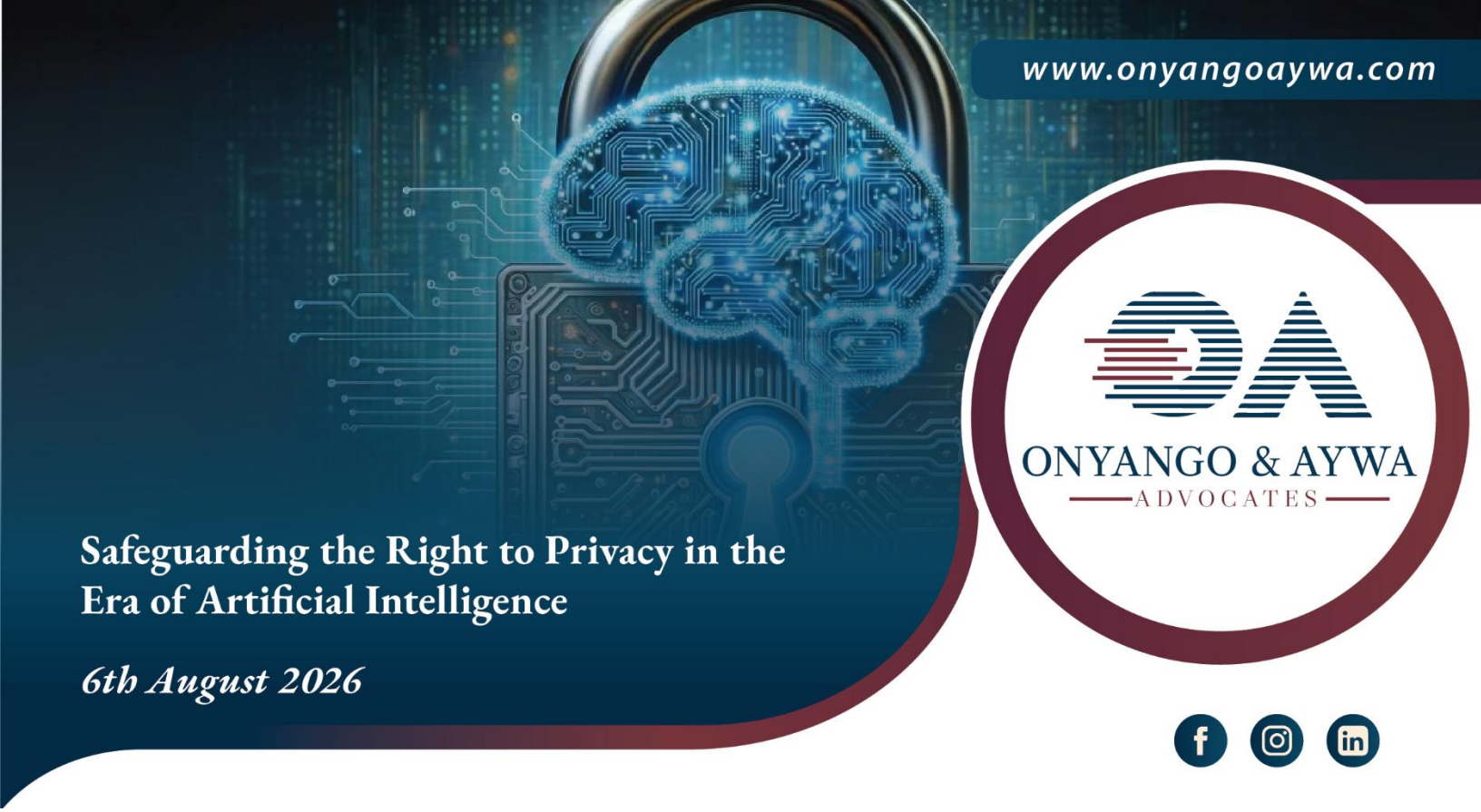

www.onyangoaywa.com

ONYANGO & AYWA
ADVOCATES

Safeguarding the Right to Privacy in the Era of Artificial Intelligence

6th August 2026

Introduction

We have all encountered hyper-realistic AI-generated images featuring recognizable faces. Some of these images have been maliciously manipulated in offensive or humiliating ways, bringing shame to individuals who had no knowledge that such portrayals could exist. Until recently, such a possibility would have seemed almost unimaginable. Yet in the present age of artificial intelligence, this has become common reality. As AI systems become more powerful and more widely used, questions arise about the privacy of personal information. *What happens when artificial intelligence is fed information that ought to remain private? Can individuals truly be secure when they have no knowledge of what information about them may have been supplied to AI systems, or how such information may later be used?*

These privacy risks multiply inside confidential, highly regulated professions, for example:

- Medical practitioners who are bound by strict statutory duties to protect patient privacy.
- Lawyers who operate under absolute rules of client-attorney privilege.

In such spaces then, new and complex questions:

1. What happens if professionals from such fields input confidential information into AI systems that are not designed to safeguard that information?
2. Could such conduct amount to a breach of professional duty, and if so, could the individuals involved be held legally liable?

The Legal Framework in Kenya

In Kenya, there are various laws that seek to protect individuals from such intrusions into their privacy. Although many of these laws were not drafted specifically with artificial intelligence in mind, Kenyan legislation has often been framed broadly enough to address emerging challenges. As a result, existing legal principles continue to offer a foundation upon which issues arising from the use of artificial intelligence can be considered and regulated.

For starters, Kenya's Constitution explicitly guarantees the right to privacy. Article 31(1) provides that "Every person has the right to privacy," including protection of one's personal information and communications. This was confirmed by Kenyan courts in the Huduma Namba case, as a broad right encompassing personal data.

The Data Protection Act (DPA) 2019, in turn, gives this right force of law: it requires all processing of personal data to be fair, lawful, and transparent. Notably, Section 35 of the DPA bans any fully-automated decision that "produces legal effects or significantly affects" a person. In other words, Kenyans cannot be subjected to solely AI decisions without human intervention, unless explicit consent is provided.

The Shifting Tide: The Artificial Intelligence Bill, 2026

While the DPA (2019) and the National AI Strategy 2025–2030 laid an important foundation, Kenya has shifted from policy ambition to definitive legislative enforcement with the introduction of The Artificial Intelligence Bill, 2026. Modeled loosely after international benchmarks like the EU AI Act, this Bill introduces a strict, risk-based classification model consisting of four tiers: unacceptable, high, limited, and minimal risk.

Importantly, the Bill introduces a new independent regulatory watchdog: the Office of the Kenya Artificial Intelligence Commissioner. This "digital sheriff" is granted wide enforcement powers to inspect AI systems, maintain a public registry of high-risk technologies, and investigate consumer complaints regarding automated bias or rights violations.

Addressing the crisis of identity theft and non-consensual synthetic media outlined in this article's introduction, the AI Bill, 2026 introduces mandatory transparency safeguards. Under the new statutory provisions:

- Any provider or deployer utilizing an AI system that generates or manipulates images, voice, or likeness (deepfakes) must secure explicit, documented consent from the affected individual or their legal representative.
- Systems that output synthetic media are required to clearly label and watermark the content as AI-generated.
- High-risk applications spanning critical sectors like healthcare, finance, and security face mandatory data protection impact assessments, leaving corporate actors open to severe administrative penalties if they breach these safe boundaries.

With the dual-watchdog system—the ODPC and the new AI Commissioner—it is aimed to ensure that the rapid uptake of AI does not come at the expense of fundamental constitutional privacy rights.

Legal and Policy Recommendations

Much has been done, and much more needs to be done. To safeguard the constitutional right to privacy amid rapid AI adoption, Kenya must transition from general guidelines to an enforceable, risk-based regulatory framework. Balancing technological innovation with robust citizen protection requires a multi-pronged approach across our legislative and corporate ecosystems.

1. Direct Regulatory and Statutory Interventions
    - Parliament should fast-track and enact the Artificial Intelligence Bill, 2026 to codify clear risk classifications. This framework must categorically ban unacceptable algorithmic practices while imposing strict, audited transparency rules on high-risk domains like banking, healthcare, and state security.
    - Kenya should fully equip the Office of the Data Protection Commissioner (ODPC) alongside the incoming Office of the Artificial Intelligence Commissioner. These bodies must be given the operational funding required to conduct mandatory, proactive algorithmic audits and enforce strict Data Protection Impact Assessments (DPIAs) before any large-scale AI system goes live.
    - Parliament should update the Computer Misuse and Cybercrimes Act (CMCA), 2018 by introducing distinct, heavy criminal penalties specifically targeting AI-generated harm, such as the weaponization of malicious deepfakes and mass automated identity theft.

2. Shift to "Privacy by Design" in Corporate Practice

- Organizations deploying AI models in Kenya must embed privacy into their tech architecture by default. This is to mean that systems should strictly collect and process only the data necessary to achieve their specific operational goals.
- Corporate operators of AI systems must implement rigid anonymization, pseudonymization, and end-to-end encryption workflows. This will ensure public-facing tools—like customer service AI chatbots and automated financial recommendation engines—never inadvertently expose sensitive user metadata or leak copyrighted data blocks.
- Companies must keep transparent, chronological logs of their AI training datasets. This operational protocol will prevent the non-consensual harvesting of unrelated personal data and insulate businesses from catastrophic regulatory fines under the Data Protection Act.

Final Thoughts

Artificial intelligence brings a huge promise for Kenya, but this rise of the "Silicon Savannah" should not happen at the expense of fundamental human rights. As global policy-makers emphasis that AI systems must respect privacy at every stage, so must the Kenya government and judiciary firmly uphold the principle that constitutional protections are non-negotiable. It is only in doing so that we shall ensure that every automated system features a clear mechanism that guarantees every Kenyan citizen the right to human intervention, explanation and legal appeal when facing an algorithmic decision.

By:

Faith Kariithi (Ms) | Lawyer ***Aywa S. (Mr) | Managing Partner***

August 6th, 2026