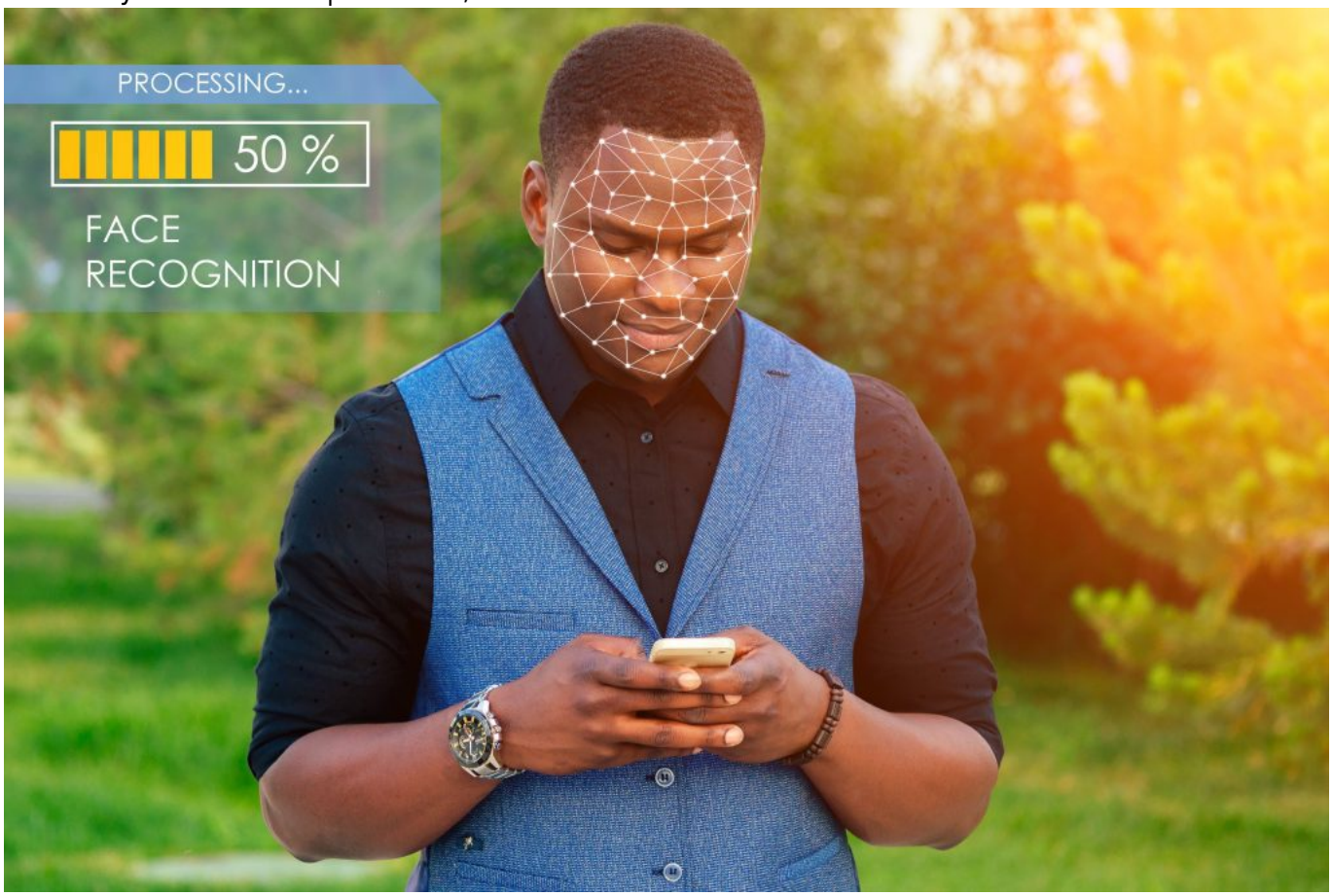
AI: THE BIOMETRIC “HONEY TRAP”

Category: Artificial Intelligence AI,Privacy Law and POPIA
written by Senelo Thaba | March 20, 2026



The Growing Use of AI Image Analysis Tools

The use of artificial intelligence (“**AI**”) tools that analyse uploaded images has increased rapidly in recent years. We have all seen social media feeds flooded with AI generated avatars, polished professional headshots, personality scores, and “future self” predictions based on a single selfie. These tools are marketed as harmless fun, innovative enhancements, or even essential for building a modern digital presence. They are widely accessible, often free or low cost, and designed to feel entertaining rather than intrusive. Yet beneath the aesthetic upgrades and playful interfaces lies a far more complex reality.

When a user uploads a photograph, they are not merely sharing a JPG file. They are submitting raw material for sophisticated data extraction. AI systems convert pixels into measurable facial patterns, behavioural predictions, and, in many cases, biometric templates. What feels like voluntary participation in “entertainment AI” is, from a legal perspective, a large-scale migration of highly sensitive personal data into privately controlled systems.

This shift marks a significant transformation in how individuals interact with technology. Personal images, once primarily shared for social connection, are now actively provided to automated systems designed to analyse, interpret, and infer information about the person depicted. To the average user, this may appear harmless, but to an attorney at PPM Attorneys, it resembles a biometric goldmine operating in an evolving and uncertain regulatory environment.

AI image analysis tools function as data-processing engines that convert visual information into

structured, machine-readable identities.[1] In South Africa, this development triggers a complex web of obligations under the *Protection of Personal Information* Act ("POPIA"). While a photograph qualifies as personal information, the moment an AI system extracts and processes unique facial features, the data may shift into the category of biometric information, which attracts heightened legal protection. This transition from ordinary personal data to special personal information fundamentally changes the compliance landscape.

Despite the rapid growth of these technologies, public understanding of their legal and practical implications remains limited. Questions surrounding consent, automated decision-making, regulatory gaps, and the interpretation of concepts such as "publicly available data" continue to create uncertainty.

From Photos to Biometric Data — The Hidden Privacy Risk

AI image analysis does far more than simply "read" a photograph; it converts it into data. Using computer vision and Convolutional Neural Networks **"CNNs"**, a system that analyse images in layers to detect patterns, shapes, and facial landmarks. When a photo is uploaded, the system maps features such as jawlines, eye spacing, and facial proportions, transforming them into what is known as a facial vector, a numerical template that allows AI systems to recognise faces, verify identities, and train facial recognition models at scale.[2] This technology already powers many everyday systems, from medical image diagnostics and banking identity verification to retail content moderation and biometric security.

The legal and privacy implications arise once that transformation occurs. Unlike ordinary personal data, biometric information cannot simply be reset or replaced. A password can be changed and an email account recovered, but the physical characteristics that make up a facial vector are permanent. Once captured and incorporated into recognition systems or training datasets, those identifiers may persist indefinitely within AI models. What appears to be a routine photo upload can therefore become the creation of a persistent digital identifier.

For users, the practical consequences are often underestimated. When AI tools analyse uploaded images, they are not merely processing photographs, they are extracting biometric identifiers that can be stored, matched, and reused. In many cases, individuals have limited visibility into how long images are retained, whether they are incorporated into training datasets, or if they are shared across platforms or third-party systems. This lack of transparency makes it difficult for users to exercise meaningful control over their own biometric information[3].

Ultimately, this creates a widening gap between user expectations and the realities of AI-driven image analysis. What feels like a harmless upload may expose highly sensitive biometric data to long-term storage, automated profiling, and unforeseen uses. For organisations deploying AI image technologies, and for individuals interacting with them, the challenge is no longer simply about data protection, but about how biometric identity itself is governed in an increasingly AI-driven digital environment.

Consent and transparency

Consent is central to data protection, but in AI image analysis, it often falls short. Users are presented with lengthy, jargon-heavy terms that rarely explain how their photos will be processed, stored, or reused. Even when formal consent is obtained, it may not be meaningful, the complexity of AI systems and the knowledge gap between users and providers makes informed decision-making difficult. This raises serious legal and ethical questions about whether current consent models are fit for purpose in biometric AI applications.

Profiling and inference risks

AI tools don't just identify faces, they can infer personal traits and characteristics, often without the user's knowledge. These inferences may be inaccurate, biased, or based on flawed assumptions, yet they can still influence how individuals are perceived or treated by automated systems. Because profiling is automated, opportunities to challenge or correct these conclusions are extremely limited. The automated nature of these processes limits opportunities for individuals to challenge or correct such inferences.

Cross-border processing and accountability

Many AI image analysis platforms operate globally. Images uploaded in one country may be processed or stored in multiple jurisdictions. This creates uncertainty regarding which legal frameworks apply and which regulators have oversight. Cross-border data flows complicate enforcement and accountability, particularly where jurisdictions offer differing levels of protection for biometric data. This means that an individual's biometric information may be subject to regulatory regimes they are unfamiliar with and cannot easily access.

Regulatory pressure

Data protection laws in many jurisdictions recognise biometric data as sensitive and deserving of enhanced protection. A good example is the General Data Protection Regulation **"GDPR".**[4] However, these frameworks were largely developed before the widespread adoption of AI-driven image analysis. The Protection of Personal Information Act[5], which was promulgated in 2013, predates many contemporary AI applications. As a result, there is often limited guidance on issues such as secondary use of images for model training, automated inference, long-term retention, and accountability for harm caused by profiling. This place increasing pressure on existing legal frameworks to adapt to technological developments.

The rapid growth of AI image analysis tools demonstrates how quickly innovation can outpace public understanding and legal clarity. What appears to be simply entertainment, or convenience often involves the extraction and processing of biometric data, the generation of inferences, and the large-scale reuse of personal images in ways that significantly alter their original purpose. The fact that images may be publicly available does not eliminate the legal, ethical, or constitutional concerns that arise when they are transformed into structured biometric identifiers and incorporated into automated systems.

The rapid adoption of AI image analysis demonstrates how innovation can outpace legal clarity. What seems like a harmless photo upload can lead to the extraction of biometric data, automated profiling, and large-scale reuse of personal images in ways far beyond the user's control. Transparency, meaningful consent, and clear accountability are no longer optional, they are essential to safeguard privacy, dignity, and autonomy in the age of AI.

---

[1] Cloudinary Guides. (2026) Breaking Down AI Image Analysis

[2] Klippa a Doxis Company. (2025) Image Processing: A Practical Guide for Businesses in 2026

[3] Science Direct. (2022) Protection of the rights of the individual when using facial recognition technology

[4] Regulation (EU) 2016/679

[5] Act 4 of 2013