WERKSMANS ATTORNEYS

REGULATORY

Error 404 – when facial recognition does not see you – a tale of how R1, R2 and R7 wages were paid for a week's work

19 December 2024 *7 min read*

Since its inception, facial recognition technology has been regarded as the future for security, safety, technology and innovation.[1] Indeed, the possibilities that arise from the usage of facial recognition technology are endless. Facial recognition technology can change law enforcement worldwide, process facial biometrics of employees in the workplace or people in large crowds, and by doing this, it becomes possible to identify employees or individuals within those crowds. However, in a similar breath, facial recognition technology has the potential to infringe on fundamental human rights, particularly the right to privacy, and if this technology is not used within the boundaries of the law, it becomes dangerous.[2]

It was recently reported[3] that several County Fair employees received single-digit salaries – R1 – due to a technical glitch that was tied to its facial recognition system used to log the check-in and check-out times of employees of County Fair. This matter represents an example of the negative consequences that can result in a world where perfection is unattainable. The fact that an employee was not paid due to a glitch in facial recognition technology highlights important questions that must be considered when it comes to the usage of facial recognition technology.

It was reported that –[4]

- on 29 November 2024, an employee of County Fair (a supplier of fresh chicken), received a notification that her wages had been deposited into her bank account only to discover that she had been paid just R2 for a week's work. The employee was expecting to be paid R1,300 and subsequently informed County Fair of the error;
- about a week later, on 7 December 2024, the same employee was expecting to receive R2,600 for two weeks' wages, but only received R7;
- it then transpired that the employee was one of several County Fair employees who received single-digit salaries which County Fair attributed to a glitch with its new facial recognition technology. Three other employees had received R1, R2 and R7 weekly wages;
- the facial recognition technology allows workers access to County Fair's factory and logs their check-in and check-out times; and
- County Fair subsequently acknowledged that the newly implemented recognition system caused errors that affected "*a small number of employees*" and lodged an investigation into what caused the error.

In terms of the Protection of Personal Information Act 4 of 2013 ("**POPIA**"), facial recognition technology is a form of biometric information which POPIA defines as "*a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition*". Biometric information is, in turn, a form of special personal information to which there is a general prohibition applicable to the processing of such (biometric) information.[5]

When it comes to the usage of facial recognition technology, POPIA must be considered holistically and this involves (but is not limited to) the following considerations –

- whether there is any applicable **general authorisation** applicable to the processing of special personal information as set out in section 27 of POPIA. Section 27 of POPIA sets out various grounds in terms whereof the prohibition on the processing of special personal information does not apply. This includes, amongst others, processing on the basis of consent or if the information has deliberately been made public by the data subject;
- how long biometric information will be **retained** for and whether such retention complies with section 14 of POPIA which provides that records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed;

- whether the usage of facial recognition technology amounts to **further processing** and, if so, whether such further processing complies with section 15 of POPIA which sets out various grounds that a responsible party can rely on to further process personal information, including if the new purpose is compatible with the original purpose, if there is consent or if the further processing is necessary to comply with an obligation imposed by law;
- whether the responsible party is able to give effect to the **rights of data subjects**, particularly the rights of objection, access and correction;
- whether the facial recognition technology gives rise to **profiling** of a data subject as a result of **automated decision making**. Section 71(1) of POPIA includes a list of examples that would be considered as "profiling" including profiles created to assess the data subject's performance at work or his, her or its credit worthiness, reliability, location, health personal preferences or conduct. It is important to note that section 71(1) of POPIA gives data subjects the right not to be subject to a decision which results in legal consequences for them or which affects them to a substantial degree, if the decision is based solely on the automated processing of personal information intended to profile the data subject. This right is however subject to certain exceptions contained in section 71(2) of POPIA which provides that the prohibition against automated decision making do not apply if the decision was taken in connection with the conclusion or execution of a contract or if the decision is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects; and
- the risk of misidentification and requirement for **data accuracy** as set out in section 16 of POPIA.

Given the various intricacies involved with the usage of facial recognition technology from a compliance perspective, a delicate balance must be achieved, balancing the usefulness of the facial recognition technology on one hand with compliance on the other hand.

Considering the usage of facial recognition technology in your business? Consider the implications carefully and always ensure that the specific facial recognition technology complies with POPIA and any other applicable legislation.

---

[1] For example, see –

- the article here wherein it is recorded that the Commissioner of the Metropolitan Police Service of London "*praise for facial recognition technology*", accessed on 11 December 2024;
- the article here wherein it is recorded that "*A trial of facial recognition technology in New Zealand has been praised as 'encouraging' as authorities attempt to curb retail crime*", accessed on 11 December 2024;
- the article here wherein it is recorded that "Police hail improved accuracy of facial recognition tech as campaigners urge ban", accessed on 11 December 2024.

[2] See Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police [2021] PER 12, available here, accessed on 11 December 2024.

[3] See the news article here, accessed on 11 December 2024.

[4] See the news article here, accessed on 11 December 2024.

[5] See section 26(a) of POPIA.



Ahmore Burger-Smidt

Head of Regulatory

View Profile



Dale Adams

Keep us close