PROFILING – AI AND PRIVACY CONSIDERATIONS

Category: Privacy Law and POPIA,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | March 10, 2023

As technologies like artificial intelligence make profiling easier, privacy regulation becomes even more important.

Profiling for purposes of security, recruitment, creditworthiness assessments and even advertising can be extremely useful to both individuals and corporates. It does however also raise serious concerns, particularly in the privacy space, if not done lawfully.

For the purposes of this article, profiling means "*the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people.*"[1]

Profiling is an essential part of businesses such as banks, which use credit worthiness assessments as one of the factors that determine whether to grant someone finance.[2] It has also become a valuable tool for organisations, for example in their internal audit and security functions.

Some organisations' internal audit departments are now using artificial intelligence tools to assist with fraud prevention, combatting crime such as corruption and for forensic examinations. There are also some which use artificial intelligence tools to proactively reduce the risk of criminal activities affecting their operations. For example, in his most recent State of the Province Address, Gauteng Premier, Panyaza Lesufi, announced Gauteng Province's plan to roll out drones and CCTV cameras that are likely to be artificial intelligence enabled.[3]

Each of these activities is likely to use people's (referred to as "data subjects" in the privacy context)

personal information to achieve their objectives. These activities can have profound consequences for the people they are directed at, such as credit refusal or criminal prosecution. The negative consequences of profiling and artificial intelligence tools were demonstrated in a case the Netherlands Government lost, where it was using an artificial intelligence tool to try to prevent social welfare fraud.[4]

In circumstances where the profiling is done using personal information collected from diverse sources, or processed by automated technology like artificial intelligence, privacy laws such as South Africa's Protection of Personal Information Act ("**POPIA**") or the European Union's General Data Protection Regulation ("**GDPR**"), have implemented protections for people.

For example, POPIA has specific provisions regulating profiling. Section 57(1) of POPIA says:

> *The responsible party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any processing if that responsible party plans to—*
>
> *(a) process any unique identifiers of data subjects—*
>
> *(i) for a purpose other than the one for which the identifier was specifically intended at collection; and*
>
> *(ii) with the aim of linking the information together with information processed by other responsible parties;*
>
> *(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;*
>
> *(c) process information for the purposes of credit reporting; or*
>
> *(d) transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72.*

What is important, is the phrase "*with the aim of linking the information together with information processed by other responsible parties*". Take the example of an organisation with CCTV cameras that are able to scan the vehicle licence plates of delivery vehicles entering its premises. If, that organisation then has access to South Africa's National Traffic Information System's ("**NaTIS**") vehicle registration data base, and uses this to verify the authenticity of such vehicles, it will need to apply to the Information Regulator for prior authorisation.

Looking to the future, consider a scenario which, until 5 years ago, seemed like science fiction. For this, we look to the Metaverse, described as "*the emerging 3-D-enabled digital space that uses virtual reality, augmented reality, and other advanced internet and semiconductor technology to allow people to have lifelike personal and business experiences online.*"[5] In this scenario, individuals wearing a mixed reality headset (which incorporates a multitude of sensors) could potentially become the subjects of highly targeted influence campaigns, based on in-depth profiling on a scale that has not been experienced before.[6]

It is therefore critical that organisations that engage in or intend engaging in profiling, ensure that they are transparent about their activities and also determine whether there is a need to obtain prior

authorisation from the Information Regulator. Organisations that do so are likely to garner more respect from the people who use, or are the subjects of, their services.

Contact us for more good, clear, precise advice.

---

[1] https://languages.oup.com/google-dictionary-en/

[2] For more on creditworthiness and related privacy matters, read the EDPS' *Opinion 11/2021 on the Proposal for a Directive on consumer credits*

[3] https://www.gov.za/speeches/address-gauteng-premier-panyaza-lesufi-during-state-province-address-gauteng-provincial

[4] See *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case*, which is available here.

[5] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse

[6] For more on this, read Louis Rosenberg's article titled *The Metaverse and Conversational AI as a Threat Vector for Targeted Influence*, found here: https://www.linkedin.com/feed/update/urn:li:activity:7033795359554367488/