African Journal on Privacy & Data Protection

To cite: T Davis & W Trott 'The regulation of artificial intelligence through data protection laws: Insights from South Africa' (2024) 1
African Journal on Privacy & Data Protection 207-219

The regulation of artificial intelligence through data protection laws: Insights from South Africa

*Tara Davis**
Senior Associate Attorney, Power & Associates, Johannesburg, South Africa

*Wendy Trott***
Senior Associate Researcher, ALT Advisory, Johannesburg, South Africa

Abstract:

The use of artificial intelligence (AI) has amplified the privacy concerns of big data in the digital era. AI systems collect personal information through covert and complex ways that may undermine consent. Data used in these systems persists indefinitely and is constantly repurposed beyond the original purposes for which consent was obtained. The ability of AI to make inferences raises the prospect of processing information about data subjects that never consented in the first place, and AI's reliance on big data incentivises behaviour that undermines the data minimisation principle common to most data protection frameworks. Despite these risks, the regulation of AI is woefully lacking in the African context. The only binding domestic legislation in most African states that addresses any form of automated decision making is data protection laws. This article explores the effectiveness of data protection laws in mitigating the risks posed by AI using the example of South Africa.

* BA (RU), LLB (UCT), LLM (Wits); tara.davis@powerlaw.africa
** BA (UGA), MA (Sciences Po Paris); wendy.trott@altadvisory.africa

Key words: data protection; artificial intelligence; privacy; data minimisation; consent

1 Introduction

Artificial intelligence (AI) has permeated the everyday activities of our lives. Beyond its use in search engines and navigation, it also creates images of Pope Francis in a puffer jacket,[1] wins art competitions,[2] and writes and directs movies.[3] It is here, and it is here to stay. It brings with it enormous potential and a significant number of risks – particularly those related to data protection and the right to privacy.

This article explores the regulation of AI through data protection legislation. First, it unpacks AI and the privacy risks it poses. Second, it examines the ways in which AI is regulated in Africa, highlighting that, at present, the only domestic legislation in most African countries that addresses AI in any way is data protection legislation. Third, it analyses the effectiveness of data protection laws in regulating AI by using South Africa's data protection law as a case study. It concludes that although data protection laws currently are the primary method through which AI is regulated on the continent, they are insufficient to protect against the extensive privacy risks posed by AI.

2 What is artificial intelligence?

There is no globally-accepted definition of AI,[4] but it is broadly accepted that AI refers to the implementation of human-like intelligence by a machine.[5] Defining AI is a challenging exercise precisely because 'intelligence' exists on a spectrum: A calculator is intelligent in that it is capable of reliably computing outcomes. The commonly-accepted difference between a calculator and AI is that the latter has intelligence on a multi-dimensional spectrum: It has scale, speed, a

1 '"It's not even real?' Social media stunned by AI image of Pope Francis wearing a stylish puffer coat' *Independent* 26 March 2023, https://www.independent.co.uk/life-style/fashion/pope-francis-ai-image-puffer-b2308159.html (accessed 30 October 2023).

2 'Art made by AI wins fine arts competition' *Impakter* 13 September 2022, https://impakter.com/art-made-by-ai-wins-fine-arts-competition/ (accessed 30 October 2023).

3 No Film School 'This film was written and directed by AI – Here's the how and what you can learn' 23 December 2022, https://nofilmschool.com/2022/12/filmmakers-use-ai-write-and-direct-short-film-and-it-actually-makes-some-sense (accessed 23 March 2023).

4 P Stone and others 'Artificial intelligence and life in 2030: One hundred year study on artificial intelligence: Report of the 2015-2016 Study Panel' September 2016 Stanford University, http://ai100.stanford.edu/2016-report (accessed 30 October 2023).

5 The society for the study of artificial intelligence and simulation of behaviour 'What is AI?' 5 September 2013, https://aisb.org.uk/what-is-ai/ (accessed 23 March 2023). Professor John McCarthy, who first coined the term, defined it as 'the science and engineering of making intelligent machines'. Standford University Human-Centred Artificial Intelligence 'Artificial intelligence definitions' (2020), https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf (accessed 30 October 2023).

degree of autonomy, and generality.[6] AI is an umbrella term – often vaguely and confusingly used – that can refer to a relatively wide range of technologies that fall somewhere on this spectrum, ranging from content-classification algorithms and speech recognition software to ChatGPT and self-directing robots.

Certain AI applications can mimic specific human-like attributes, such as language processing or speech recognition. AI uses certain techniques, one of which is machine learning, which uses training data to teach systems to accurately solve a specified problem in a given domain.[7] These techniques are currently used to develop and implement artificial *narrow* intelligence and are evident in current uses of AI.[8] For example, AI-powered content classification programmes may take an image as *input* and produce as an *output* the probability that the image is that of South African President Cyril Ramaphosa. The AI programme is accordingly trained on large data sets – in this case, images that are either of President Cyril Ramaphosa or not. As noted by the Information Commissioner's Office of the United Kingdom,[9] '[t]his may not sound very different from standard methods of data analysis. But the difference is that AI programmes don't linearly analyse data in the way they were originally programmed. Instead, they learn from the data in order to respond intelligently to new data and adapt their outputs accordingly.'

Large data sets, therefore, are crucial for the development of AI programmes – their training requires a large amount of varied data.[10] AI programmes exist in a 'complex, interdependent, global data ecosystem'[11] in which AI-produced outputs can also be used as new input data for further AI training models.[12] AI has also been enabled by the development of 'big data technologies' such as improved computing storage capabilities and super-fast processing machines in recent years,[13] facilitating the collection and processing of previously inconceivably large quantities of data. It is for this reason that AI is closely associated with 'big data,'[14] a term used to describe 'the explosion of available information.'[15]

6 Stone and others (n 4).
7 Media Monitoring Africa 'The implications of artificial intelligence on information rights' November 2021, https://mediamonitoringafrica.org/wordpress22/wp-content/uploads/2022/10/Media-Monitoring-Africa-Discussion-Document-on-AI.pdf (accessed 28 March 2023).
8 At present, artificial general intelligence, a term that refers to a machine's ability to complete several tasks at a level at least equivalent to that of a human across multiple domains, has not yet been developed.
9 Information Commissioner's Office 'Big data, artificial intelligence, machine learning and data protection' v2.2. 8, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (accessed 23 March 2023).
10 L Mitrou 'Data protection, artificial intelligence and cognitive services: Is the General Data Protection Regulation (GDPR) "artificial intelligence-proof"?' *SSRN* 31 December 2018 7, https://ssrn.com/abstract=3386914 (accessed 28 March 2023).
11 L McGregor, D Murray & V Ng 'International human rights law as a framework for algorithmic accountability' (2019) *British Institute of International and Comparative Law* 310.
12 As above.
13 R Kune and others 'The anatomy of big data computing' (2015) 46 *Journal of Software: Practice and Experience* 79-105.
14 Information Commissioner's Office (n 9) 6.
15 J Fan, F Han & H Liu 'Challenges with big data analysis' (2014) 1 *National Science Review* 293.

3 Privacy risks posed by artificial intelligence

Because of the necessarily close relationship between AI and big data, its use raises serious privacy concerns on several vectors.[16] The right to privacy is enshrined in article 12 of the Universal Declaration of Human Rights (Universal Declaration) and article 17 of the International Covenant on Civil and Political Rights (ICCPR), and it is recognised as an enabler of other fundamental human rights. The right to privacy has undergone significant change in the digital era as new technologies have developed. Inherent in the modern conception of the right is the recognition that 'individuals should determine what information about themselves is made public[17] and control how that information is collected and used'.[18] This implies informed consent and knowledge of what one's data is used for.

AI forms the backbone of search algorithms, recommendation engines and facial recognition systems. Many of these systems collect extensive personal information, such as email addresses, pregnancy status, or pictures of one's face, and use it to influence behaviour by, for example, recommending a particular movie or an ante-natal vitamin[19] or influencing students' behaviour or attendance at school.[20] In some instances, AI is used to scrape text content on the internet to fuel generative AI chatbots.[21] Scraping is just one of several new and increasingly-covert methods used to collect users' information online.[22] This raises serious questions about whether meaningful consent is or can be obtained in such cases. Data used in AI systems also persists indefinitely and is constantly repurposed for use beyond its original purposes, undermining a data subject's ability to understand how and why it is used.[23]

In addition to data that is collected directly from data subjects, AI is also capable of analysing large quantities of observed, derived and inferred data, and, as a result of the latter, making inferences and predictions far beyond human

16 S Dilmaghani and others 'Privacy and security of big data in AI systems: A research and standards perspective' (2019) *IEEE*.
17 D Milo & P Stein *A practical guide to media law* (2013) 51.
18 J Neethling 'Die reg of privaatheid' LLD thesis, UNISA, 1976 358.
19 C Duhigg 'How companies learn your secrets' *New York Times Magazine* 16 February 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp (accessed 20 November 2023).
20 J Karoub 'U-M study finds facial recognition technology in schools presents many problems, recommends ban' 10 August 2020, https://news.umich.edu/u-m-study-finds-facial-recognition-technology-in-schools-presents-many-problems-recommends-ban/ (accessed 20 November 2023); M Andrejevic & N Selwyn 'Facial recognition technology in schools: Critical questions and concerns' (2019) 45 *Learning, Media and Technology* 115.
21 'ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned' *The Conversation* 10 February 2023, https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283 (accessed 28 March 2023).
22 Mitrou (n 10) 22.
23 Mitrou (n 10) 20.

capacity and traditional data protection conceptions.[24] Provided with only a small amount of data, AI can generate or infer new data about existing data subjects as well as those that did not originally provide their data.[25] The ability to withdraw consent for such use is challenging after data has been incorporated into an AI system.[26] The use of large quantities of data to feed AI systems can also make real anonymisation impossible or enable the re-identification of anonymised data,[27] with the ability to infer the identity of data subjects that have not provided consent for such based on a combination of data points.

Advanced data analysis and AI tools are used to act on these inferences by influencing people's behaviour in some benign ways – such as making movie recommendations – and those that are more concerning – such as electoral decisions and automated disinformation.[28] Is there consent when data subjects have little understanding of what inferences are being developed about them and how they are being targeted or influenced based on those inferences?

More generally, AI has incentivised a culture of collection in which the maximum amount of data is sought to meet the needs of 'big data', as discussed above.[29] For example, AI is used to feed digital advertising algorithms with micro-targeted data collected on a mass scale, monetising the most personal and private aspects of a user's life such as personality traits, cell phone history and emotional states.[30] This raises questions about the violation of the data minimisation principle that is a widely-accepted element of the right to privacy in the digital age.[31]

As pointed out by the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinions and Expression:[32]

> Because AI systems work by exploiting existing datasets and creating new ones, the ability of individuals to know, understand and exercise control over how their data are used is deprived of practical meaning in the context of AI. Once data are

24 Media Monitoring Africa 'The implications of artificial intelligence on information rights' November 2021, https://mediamonitoringafrica.org/wordpress22/wp-content/uploads/2022/10/Media-Monitoring-Africa-Discussion-Document-on-AI.pdf (accessed 28 March 2023).

25 B Lepri, N Oliver & A Pentland 'Ethical machines: The human-centric use of artificial intelligence' (2021) 24 *iScience* 102249.

26 E Fosch Villaronga, P Kieseberg & T Li 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten' (2018) 34 *Computer Law and Security Review* 304-313.

27 K Manheim & L Kaplan 'Artificial intelligence: Risks to privacy and democracy' (2018) 21 *Yale Journal of Law and Technology* 106.

28 N Bontridder & Y Poullet 'The role of artificial intelligence in disinformation' (2021) *Data and Policy* 1.

29 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, United Nations General Assembly, A/73/348 29 August 2018 11.

30 Manheim & Kaplan (n 27).

31 AC Raul, F Blythe & S Porath Rockwell 'Privacy by design and data minimisation' (2022) *Global Data Review* 13.

32 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 29).

repurposed in an AI system, they lose their original context, increasing the risk that data about individuals will become inaccurate or out of date and depriving individuals of the ability to rectify or delete the data.

Once fed into AI systems, data can be reused and repurposed, and take on a life of their own. It is unclear how and to what extent the quality and correctness of personal information that has been used in such a system can be maintained over the longer term. Biased, poor-quality, or outdated underlying data can also affect AI's outputs. This may compromise other rights such as equality and freedom from discrimination when AI[33] is used to make consequential decisions about a person such as their likelihood of recidivism.[34] The significant data disparities that exist, particularly in Africa, mean that unrepresentative or inaccurate training data is a major concern for data subjects' consent and control over the use of their information.[35]

As the deployment of AI rapidly progresses across the African continent,[36] it becomes increasingly necessary and urgent to evaluate the steps that are being taken to regulate these technologies and guard against the privacy risks they pose.

4 Artificial intelligence governance in Africa

Research reveals that disturbingly few measures have been implemented to govern the deployment of AI in Africa.[37] Regulation may mean a range of interventions, from behavioural control and self-regulation through to legislation.[38] There have been several developments in Africa in recent years of normative self-regulation programmes and principles by civil society, academics and international and continental organisations. For example, in 2021 the African Commission on Human and Peoples' Rights (African Commission) adopted Resolution 473 on the need to undertake a study on human and peoples' rights and artificial intelligence (AI), robotics, and other new and emerging technologies in Africa.[39]

33 European Union Agency for Fundamental Rights 'Bias in algorithms – Artificial intelligence and discrimination' 8 December 2022, https://fra.europa.eu/en/publication/2022/bias-algorithm (accessed 28 March 2023).

34 M Farayola and others 'Fairness of AI in predicting the risk of recidivism: Review and phase mapping of AI fairness techniques' (2023) ARES 2023: The 18th International Conference on Availability, Reliability and Security.

35 P Gehl Sampath 'Governing artificial intelligence in an age of inequality,' (2021) 12 *Global Policy Special Issue: Digital Technology and the Political Determinants of Health Inequities* 21-31.

36 A Gwagwa & E Kraemer-Mbul 'Artificial intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions' (2020) 25 *African Journal of Information and Communication* 1-28.

37 ALT Advisory 'AI governance in Africa' September 2022, www.ai.altadvisory.africa (accessed 28 March 2023). The research reviewed six indicators of AI governance, which included dedicated AI legislation, rights regarding automated decision-making in data protection legislation, national AI strategies; draft policies or white/green papers on AI; the establishment of an expert commission or similar entity; and whether AI is a priority in the country's current National Development Plan.

38 S Chesterman *We, the robots?* (2021) 3-4.

39 African Commission on Human and Peoples' Rights Resolution on the need to undertake a study on human and peoples' rights and artificial intelligence (AI), robotics and other new and

However, both these non-binding guidelines and existing African regional human rights law frameworks are ill-equipped to deal with the complexity of AI and its potentially significant consequences for individual and collective privacy rights.[40] For present purposes, we therefore focus on the need for domestic legislation due to its uniquely-binding and authoritative nature in the domestic context.

Out of the 55 African countries,[41] only one – Mauritius – has legislation that meaningfully deals with AI, although it only applies to the financial sector.[42] Only seven countries have a national AI strategy[43] and only Tunisia has a draft policy on AI.[44] There has been a rise in the establishment of expert bodies – 13 countries have established some form of taskforce to deal with AI concerns[45] – and the publication of AI strategies that flag the need to address the ethical and rights implications of AI through improved legislation.[46] However, the dearth of regulation through binding dedicated legislation on AI has meant that data protection laws have become the most common default form of regulation in Africa at the domestic level.

---

emerging technologies in Africa ACHPR/Res. 473 (EXT.OS/ XXXI) 2021 2021, https://achpr.au.int/en/adopted-resolutions/473-resolution-need-undertake-study-human-and-peoples-rights-and-art (accessed 31 October 2023).

40 Z Xaba 'Governing artificial intelligence under the African human rights system: Drawing lessons from international best practices' LLM dissertation, University of Pretoria, 2021; L Lane 'Clarifying human rights standards through artificial intelligence initiatives' (2022) 71 *ICLQ: British Institute of International and Comparative Law* 915-944.

41 Our research focused on the 55 current African Union member states.

42 In 2021 the Financial Services Commission issued rules related to robotic and artificial intelligence enabled services, under the Financial Services (Robotic and Artificial Intelligence Enabled Advisory Services) Rules. The rules regulate licensing procedures for entities that provide investment and portfolio management services enabled by artificial intelligence. One of the compliance requirements for licensees – under sec 10(1) – is to ensure that adequate policies and controls are in place to ensure that algorithms perform as intended and for the design, testing, and monitoring of algorithms. Sec 13 also provides for the submission of independent evaluation reports on algorithms and software systems, and sec 12 requires licensees to retain details of all algorithms and software used.

43 These are Algeria, Benin, Egypt, Morocco, Sierra Leone, Mauritius and Uganda. Note that an AI strategy is defined differently to an AI policy or white paper.

44 'Tunisie: Quatre ministères se mobilisent en faveur de l'Intelligence artificielle' *Challenges* 21 February 2022, https://www.webmanagercenter.com/2022/02/21/480963/tunisie-quatre-ministeres-se-mobilisent-en-faveur-de-lintelligence-artificielle/ (accessed 29 March 2023).

45 These include Algeria, Benin, Egypt, Ethiopia, Kenya, Mauritius, Morocco, Namibia, Nigeria, Rwanda, Sierra Leon, South Africa, Tunisia and Uganda.

46 Eg, the Mauritius National AI Strategy calls for government to 'ensure a conducive environment [for AI] through a robust and yet friendly regulatory, ethics and data protection environment', touches on the complexity of enabling accountability in the use of AI, calls for the establishment of a permanent committee on ethics to maintain dialogue and formulate proposals, posits the possible need for amendments to data protection legislation to address AI, and highlights the need for a 'clear, explicit, and transparent code of ethics' on AI. See Mauritius Artificial Intelligence Strategy November 2018 4 & 67, https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf (accessed 22 February 2023). Egypt's National AI Strategy proposes the creation of a dedicated track for the National Council for Artificial Intelligence on AI ethics that includes a mandate to develop appropriate legislation and regulations and publish guidelines for the Responsible and Ethical Development of AI. See National Council for Artificial Intelligence 'Egypt Artificial Intelligence Strategy' 23 & 38, https://mcit.gov.eg/Upcont/Documents/Publications_672021000_Egypt-National-AI-Strategy-English.pdf (accessed 22 February 2023).

As of March 2023, 38 African countries have data protection laws either in force or in draft form.[47] Data protection laws provide a natural foundation for AI regulatory frameworks.[48] This is so because AI applications often *process* personal information as defined in most data protection laws. They do so in two ways:[49]

> [Personal information] can be used in the creation of datasets which are subsequently used to train AI machine-learning systems to construct algorithmic models; and conversely, such algorithmic models can be applied to datasets of personal information in order to draw inferences pertaining to particular individuals.

In light of this, several countries explicitly include automated processing within the scope of application of their data protection laws. Where they apply, automated processing of personal information must consequently comply with the requirements for lawful processing as specified in data protection laws. Notably, this would include compliance with common requirements such as data minimisation, consent and purpose specification. While AI can in many ways be implemented in compliance with these principles, on the surface, some of these principles seem at odds with the operation of AI.[50]

For example, purpose specification becomes challenging in a system that is designed to constantly iterate on inputs to generate new findings and which learns over time to complete new tasks. As such, this also raises concerns about consent. What is meaningful consent in a context in which uses are still undefined at the point of collection and when inferences are made to generate new data? AI, therefore, has fundamentally reshaped the scope of key data protection principles, including access and control.[51]

Thirty of the draft or in-force data protection laws in Africa contain a provision explicitly dealing with automated decision making as it relates to personal information.[52] Many of these closely resemble one another. In general, they create a right for data subjects not to be subject to certain types of automated decisions. These are either legal decisions intended to evaluate aspects of a person's personality, and/or decisions with other legal effects based solely on

47 ALT Advisory 'Data protection Africa', https://dataprotection.africa/ (accessed 20 March 2023).

48 K Crawford and others 'AI Now 2019 Report' December 2019 *AI Now Institute*, https://ainowinstitute.org/AI_Now_2019_Report.html (accessed 24 March 2023).

49 P Bhagattjee, A Govuza & L Sebanz 'Regulating artificial intelligence from a data protection perspective – Lessons from the EU' *Without Prejudice* December 2020, https://www.withoutprejudice.co.za/free/article/7172/view (accessed 28 March 2023).

50 European Parliament 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' European Parliamentary Research Service June 2020 5, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed 27 March 2023).

51 Research ICT Africa 'AI in Africa: Regional data protection and privacy policy' Policy Brief 3 December 2019 4, https://researchictafrica.net/wp/wp-content/uploads/2020/11/RANITP2019-3-DataProtection.pdf (accessed 24 March 2023).

52 Algeria, Angola, Benin, Botswana, Burkina Faso, Cabo Verde, Republic of Congo, Côte d'Ivoire, Eswatini, Gabon, Ghana, Guinea, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, Rwanda, São Tomé and Príncipe, Senegal, South Africa, Togolese Republic, Tunisia, Uganda, Zambia and Zimbabwe.

automated data processing intended to profile a person or evaluate aspects of their personality or behaviour.

Some laws go further than this. Botswana's Act 32 and Morocco's Law 09-08 mandate data controllers to notify the regulator before carrying out automated processing with personal information,[53] and others address the principle of 'explainability'.[54]

Benin's Law 2009-09 arguably goes the furthest. It stipulates that automated processing that is likely to exclude persons from the benefit of a right, service or contract or that includes assessments of people's social difficulties requires prior approval from the data protection authority.[55] It also requires responsible parties to notify data subjects that automated decision making has occurred, and to provide information regarding its underlying logic, significance and anticipated consequences.[56] It further provides for a public list of automated processing procedures in use.[57]

Although regulating AI through domestic legislation is a difficult task, some of the leading jurisdictions, such as the United States and Europe, have begun to coalesce around the importance of attempting to do so alongside a series of norms that should govern such efforts.[58] Africa is falling behind in these efforts.

5 South Africa's data protection law and artificial intelligence

The Protection of Personal Information Act 4 of 2013 (POPIA), South Africa's data protection law, contains several data protection principles that are common among other African states' laws.[59] These include, for example, the data subject's consent; the lawfulness of processing; and data minimisation, among others.

In light of the potential tension between data protection principles and the operation of AI, we assess whether South Africa's data protection law, by way of example, provides sufficient safeguards against the privacy-related risks posed by AI by assessing three specific issues, namely, inferred personal information, de-identification, and automated decision making.

53 Botswana Act 32 art 34; Morocco Law 09-08 art 14.
54 Eg, Cabo Verde's Law 133/V/2001 art 12(1)(c) provides that data subjects have the right to know the logic involved in any automatic processing of data concerning them; art 23 of Madagascar's Law 2014-038 on the Protection of Personal Information provides that data subjects have the right to receive information that enables them to know and contest the logic underlying any automatic processing that is used to make a decision about them that produces legal effects; and secs 23(2)(e); 34(2)(a); 37(2)(h) and 38 of the Mauritius Data Protection Act 2017 provide various rights related to automated processing.
55 Sec 407.
56 Secs 415, 416 & 437.
57 Sec 439.
58 Chesterman (n 38) 9.
59 I Ademuyiwa & A Adeniran 'Assessing data protection and privacy in Africa' (2020) *Assessing Digitalisation and Data Governance Issues in Africa* 4-6.

In this regard, it is notable that POPIA defines automated means as 'any equipment capable of operating automatically in response to instructions given for the purpose of processing information'.[60] POPIA explicitly includes the processing of personal information by automated means within its scope of application.[61] The two typical ways in which AI processes personal information – to develop datasets to train AI systems and to analyse and interpret the datasets – constitute 'processing' under POPIA. Processing is defined to mean 'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information', and the definition notes a list of activities that includes 'collection', 'collation', 'use' and 'merging'.[62] Accordingly, the processing of personal information by AI systems should, in certain circumstances, comply with the provisions of POPIA. However, POPIA is silent on several unique challenges posed by AI, as discussed below, making its application clumsy and uncertain in many ways.

5.1 Inferred personal information

As discussed, AI models can be applied to personal information to infer new information about a data subject.[63] For example, a data subject's online shopping history may be analysed to infer their gender. This is new information – but does it constitute new, distinct personal information for the purposes of POPIA? This question has obvious implications for how the information may be lawfully processed. It also raises practical questions about a data subject's control of their information – how can a data subject exercise meaningful control over personal information of which they are unaware? Further, the inference by AI is only a probable one. This implies that it will be wrong in a set number of instances, depending on the error rate, which may undermine the principles of data quality. POPIA is silent on the status of such inferred information, and accordingly it is unclear how it should be treated.

5.2 De-identification

POPIA does not apply to information that has been de-identified.[64] However, AI and the proliferation of data have made it much easier to re-identify anonymised data by linking it with, or drawing probable inferences based on additional data.[65]

60 Sec 3(4) POPIA.
61 Sec 3(1) POPIA.
62 Sec 1 POPIA.
63 European Parliament 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' *European Parliamentary Research Service* June 2020 50, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed 27 March 2023).
64 Sec 6(1)(b) POPIA.
65 European Parliament (n 63).

POPIA goes some way towards accounting for this through the definition of de-identification, which requires the deletion of information that 'can be used or manipulated by a *reasonably foreseeable* method to identify the data subject'; or 'can be linked by a *reasonably foreseeable* method to other information that identifies the data subject'.[66] However, POPIA is silent on the threshold for these requirements. A responsible party may not itself have the technological capacity or methods to re-identify such data, but a third party might. Once shared, it may be re-identified, with or without the knowledge of the responsible party, with serious consequences for the rights of the data subject. Accountability in such instances would also be challenging, raising questions with regard to both the responsible party and the party that ultimately implemented the re-identification. Further, it is not clear whether the mere existence of AI's capacity to re-identify data makes it *reasonably foreseeable* that any and all de-identified data could theoretically be re-identified. POPIA currently does not address the challenges that AI poses to de-identified information, making its definition and application uncertain.

5.3 Automated decision making

Section 71 of POPIA is the only provision that explicitly deals with processing conducted by AI. This provision provides:[67]

> (1) Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her, or it, or which affects him, her, or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

Positively, the provision aims to mitigate the risks associated with profiling by AI. However, its wording is broad and unclear and, to date, South Africa's Information Regulator has neither released guidelines on its application, nor have any codes of conduct been published.[68] It accordingly is unclear what types of decisions would be considered to affect a data subject to a *substantial degree*, what the meaning of a *profile* is, and what the threshold for *solely* requires. For example, it is unclear whether a decision would be compliant if a human reviewed and confirmed a decision after it had been made by automated means.

66 Sec 1 POPIA, as included in the definition of 'de-identify'.
67 The right is provided for in sec 5(g) and expanded upon in sec 71 of POPIA.
68 In terms of *GG* 44459, https://inforegulator.org.za/wp-content/uploads/2020/07/20210416-gg44459gen209-POPIA-CoC-CBA.pdf and *GG* 44690, codes of conduct have been compiled for the Banking Association South Africa and the credit Bureau, but they have not been published.

In addition, the provision is narrowly circumscribed in sub-section 2, which provides that the provisions do not apply in certain circumstances relating to the conclusion of contracts and where a code of conduct has been developed.

The potential risks to a data subject's rights are further exacerbated by the lack of notification provisions. POPIA does not place an obligation on the decision maker to notify a data subject that they have been subjected to a decision that was based solely on automated decision making.[69] This oversight renders the right ineffective – without knowing it has occurred, a data subject will be unable to exercise or protect their right. This is particularly so in light of recent research[70] that found that existing mechanisms in data protection law – the right to access information[71] – proved ineffective when trying to ascertain how a data subject's personal information was being used for automated processing. The research found that some of the largest companies are unable to meaningfully respond to data subjects' requests to understand whether and how their personal information is used in automated processing and whether this is in line with the provisions of POPIA.

These examples demonstrate that some of the challenges posed by AI have not been effectively resolved in South Africa's data protection law. Arguably, such findings would likely also apply to the data protection laws of other African countries that contain comparable provisions.

6 Conclusion

Data protection laws can provide some mitigation against the risks posed by AI. By incorporating AI within their scope, a degree of compliance with minimal data protection standards is ensured. However, certain data protection measures are undermined by a lack of consideration for the unique attributes of AI – particularly new and complex ways of collecting data, the creation of inferred data, and the ability to re-identify data. Further analysis is necessary to examine the possible incongruence between AI and certain data protection principles – especifically data minimisation, purpose specification, and consent – as they are embodied in many data protection laws across the African continent.

It is clear that African states must urgently take meaningful steps to address the governance lacuna in which AI is rapidly developing and which threatens a wide array of internationally and domestically-recognised human rights,

69 G Katzav 'Has POPIA adequately prepared people to exercise their right not to be subject to automated decision-making?' (2022) *De Rebus*, https://www.derebus.org.za/has-popia-adequately-prepared-people-to-exercise-their-right-not-to-be-subject-to-automated-decision-making/ (accessed 27 March 2023).

70 ALT Advisory 'Failure to access' *ALT AI*, https://ai.altadvisory.africa/wp-content/uploads/Failure-to-Access-AI-transparency-in-South-Africa-2022.pdf (accessed 24 March 2023).

71 Provided for in sec 5(g) of POPIA.

most notably the right to privacy. Further research into interpretations given in other jurisdictions, such as the European Union (EU) under the General Data Protection Regulation, to some common concepts that remain undefined in South African law, such as a *profile* and *processing based solely on automated means,* would assist to provide greater legal clarity. More research is needed to meaningfully regulate AI and provide effective protection for privacy and other rights.