REGULATING AUTOMATED DECISION-MAKING: AN ANALYSIS OF SECTION 71 OF POPIA AND ITS IMPLICATIONS FOR PRIVACY AND DATA PROTECTION

https://doi.org/10.29053/pslr.v18i1.5156

by Caitlin Leipsig

Abstract

The rapid evolution of technology and its integration into various sectors of society has necessitated comprehensive data protection legislation to safeguard individuals' privacy rights. This paper conducts a comparative analysis between the Protection of Personal Information Act (POPIA) of South Africa and the General Data Protection Regulation (GDPR) of the European Union, focusing particularly on their regulatory frameworks concerning automated decision-making and its implications for privacy and data protection. POPIA, enacted in 2013 after seven years of development, seeks to regulate the processing of personal information within South Africa, aligning with international data protection standards. However, with the emergence of automated decision-making systems powered by artificial intelligence and machine learning algorithms, concerns arise regarding privacy, transparency, and accountability. This paper explores how POPIA's principles, including accountability and data processing conditions, address these challenges, while also acknowledging potential gaps. Drawing parallels with the GDPR — recognised as the international benchmark for data protection — reveals areas where POPIA could enhance its regulatory approach. The GDPR's emphasis on transparency, explicit consent, and the right to explanation in ADM processes provides valuable insights for POPIA's refinement. Furthermore, the GDPR's provisions for regulatory strategies, codes of conduct, and remedies offer potential avenues for strengthening POPIA's enforcement mechanisms. By evaluating the foundational concepts and core values of both legislations, this paper

offers recommendations for aligning POPIA more closely with GDPR best practices, particularly in the context of ADM. It underscores the importance of continuous adaptation and international collaboration in addressing the evolving challenges of data protection in the digital age.

1 Introduction

In November of 2019, high-profile tech entrepreneur David Hansson publicly criticised the recently released Apple credit card for being sexist — claiming that his female partner had received a lower Apple Card credit limit simply for being a woman.[1] Hansson questioned why his wife — who had a better credit score and other factors in her favour — was denied her application for an increase in credit limit. Steve Wozniak, original co-founder of Apple, responded to Hansson's tweet with a similar account.[2] According to Wozniak, he received ten times the credit limit that his wife received despite the couple having no separate bank or credit accounts, or owning separate assets.[3]

Hansson was particularly critical of the fact that the credit card division representatives at Apple had no insight into how the algorithms had come to a decision and had seemingly followed the result of the algorithm blindly.[4] In another tweet, Hansson stated: [5]

> Apple has handed the customer experience and their reputation as an inclusive organization over to a biased, sexist algorithm it does not understand, cannot reason with, and is unable to control. When a trillion-dollar company simply accepts the algorithmic overlord like this ...

The 'black box' problem that Hansson described in his tweets is a notable concern in the emerging artificial intelligence (AI) sector.[6] A black box is an AI system whose inputs and operations are not visible to the user or another interested party — it arrives at decisions without explaining how they were reached.[7] Although the United States regulators exonerated Apple and its bankroller, Goldman Sachs, of breaking fair lending laws,[8] the issue that was brought up remains

1 The New York Times 'Apple Card investigated after gender discrimination complaints' https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html (accessed 10 November 2023).
2 As above.
3 As above.
4 As above.
5 As above.
6 UM-Dearborn 'AI's mysterious "black box" problem, explained' https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained (accessed 10 November 2023).
7 TechTarget 'WhatIs.com' https://www.techtarget.com/whatis/definition/black-box-AI#:~:text=Black%20box%20AI%20is%20any,to%20how%20they%20were%20reached (accessed 10 November 2023).
8 The Verge 'The Apple Card doesn't actually discriminate against women, investigators say' https://www.theverge.com/2021/3/23/22347127/goldman-sachs-apple-card-no-gender-discrimination (accessed 10 November 2023).

relevant, and it poses the question of how risks inherent in artificial intelligence and automated decision-making (ADM) affect people's day-to-day lives.[9] Many jurisdictions around the world are in the process of supplementing their existing laws to regulate artificial intelligence. These existing laws primarily occur within legislation that governs data protection — such as the European Union's renowned General Data Protection Regulation,[10] or South Africa's own Protection of Personal Information Act (POPIA).[11]

POPIA is the comprehensive data protection statute of South Africa, which seeks to regulate the processing of personal information in private and public spheres.[12] The Act, which took seven years to become fully implemented after being signed into power in 2013, sets out the minimum standards concerning the accessing and processing of personal information belonging to a data subject.[13] POPIA was created to conform with the former benchmark for data protection laws, namely the 1995 General Data Protection Directive — although this directive has since been replaced with the General Data Protection Regulation (GDPR). POPIA sets out to establish mechanisms that are in harmony with international regulations to protect the privacy of personal information.[14]

The right to privacy is fundamental, especially in today's society, with new, emerging technologies that threaten an individual's rights and freedoms in this regard. Privacy is recognised as a personality interest by the South African common law,[15] and the South African Constitution additionally recognises it in section 14.[16] Privacy is defined as:[17]

> the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

Since the 1970s, it has been put forward that an individual should be able to decide for themselves whether their personal information can be collected and used by others.[18] However, as technologies have advanced and individuals' internet usage has increased, personal

9 Automated decision making is defined in section 71(1) of the Protection of Personal Information Act 4 of 2013 as a decision that results in legal consequences for a data subject or which substantially affects them, which is based solely on the basis of the automated processing of personal information intended to create a profile of that person.
10 General Data Protection Regulation of 2016 (Regulation (EU) 2016/679).
11 Protection of Personal Information Act 4 of 2013.
12 As above.
13 Chapter 3 POPIA.
14 Roos 'Data privacy law' in van der Merwe (ed) *Information and Communications Technology Law* (2021) 515.
15 Roos (n 14) 470.
16 The Constitution of the Republic of South Africa, 1996.
17 Roos (n 14) 395.
18 Roos (n 14) 358.

information has become readily available online for use by various entities.[19] Personal data is now a valuable economic commodity for companies like Apple, Google, Facebook and others, who have built business models based on collecting and processing people's personal data to create economic income.[20]

'Big Data' is the term used to describe the practice of collecting, analysing, packaging and selling data by enterprises to ascertain the habits, personalities, and market behaviours of data subjects.[21] This practice involves combining large volumes of diversely sourced data and then analysing it through automated, self-learning algorithms to make or inform decisions.[22] The predictive potential of Big Data holds much value for companies. Initially, this monitoring of human behaviour was to increase companies' digital advertising income.[23] However, the practice has evolved into companies using the data to control exceedingly high market capitalisation values — higher than any other company in recorded history.[24]

The initial optimism of this potential has fallen away to reveal evidence of manipulation and privacy risks for data subjects.[25] It is evident that the processing of one's personal information poses a real threat to that individual's privacy,[26] and Krzystofek writes that the projection of behaviours and characteristics of persons which are modelled on uncertain information — obtained from places such as social networking services, processed through 'oversimplified algorithms defined by various institutions' — could lead to the discrimination and stigmatisation of data subjects.[27]

The rapid advancements in technology have led to the widespread use of automated decision-making systems across various industries. These systems, powered by artificial intelligence and machine learning algorithms, can analyse vast amounts of data, and make decisions without human intervention. While automation brings efficiency and convenience, it also raises privacy and data protection concerns. This article aims to explore the regulatory framework of automated decision-making under Section 71 of the Protection of Personal Information Act (POPIA) and analyse its implications for privacy and data protection.

19 Snail ka Mtuze & Papadopoulos 'Privacy and data protection' in Papadopoulos & Snail ka Mtuze *Cyberlaw@SA* (2022) 308.
20 Roos (n 14) 388.
21 Roos (n 14) 391.
22 Snail ka Mtuze & Papadopoulos (n 19) 308.
23 As above.
24 As above.
25 As above.
26 Roos (n 14) 394.
27 Krzystofek *General Data Protection Regulation (EU) 2016/679 — Post Reform Personal Data Protection in the European Union* (2019) 175.

The discussion that follows will explore the use of algorithms and AI in automated decision-making and the profiling of data subjects in specific sectors. These concepts will determine whether POPIA sufficiently allows data subjects to exercise their right not to be subject to ADM under specific conditions. Section 2 will delve into the critical elements of POPIA, defining relevant terms and examining its effectiveness. Section 3 will discuss the respective European law that governs data protection, looking at its principles and the differences between this law and the South African legislation. Section 4 will conclude the research.

1.1 Data processing and AI in Africa

Technology is not neutral, and developments such as artificial intelligence contain inherent biases that have the potential to magnify discrimination in the systems where they are implemented.[28] This potential is only intensified in developing regions.[29] The use of artificial intelligence in data processing, specifically in the Financial Services Industry, will be looked at in order to understand the context of data subjects within developing countries. It will focus on what AI and skewed data mean for the privacy and protection of data subjects in Africa. Various sources are discussed and analysed for a balanced view of the challenges addressed.

1.2 Artificial intelligence and accountability

Artificial intelligence (AI) is a broad term for a computer or software system which has the capability of being programmed to 'think' like a human in order to analyse information or data, search for patterns, or make decisions.[30] AI is being progressively more utilised as an emerging technology in various sectors, and among its core features are algorithmically controlled automated decision-making systems.[31] As discussed above, ADM systems are increasingly used in decision-making processes in both the public and private spheres.[32] These systems, while having the ability to make decisions concerning outcomes relating to matters such as health and finance, have the potential to have a significant negative impact on organisations,

28 Ahmed 'A gender perspective on the use of Artificial Intelligence in the African FinTech Ecosystem: Case studies from South Africa, Kenya, Nigeria, and Ghana' 2021 *Paper presented at International Telecommunications Society (ITS) 23rd Biennial Conference* 2.

29 Ahmed (n 28) 2.

30 ALT Advisory, A.I.MPACT, September 2022, accessible at ai.altadvisory.africa (accessed 10 November 2023).

31 Gwagwa, Kraemer-Mbula, Rizk, Rutenberg & de Beer 'Artificial Intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions' 2020 T*he African Journal of Information and Communication (AJIC) 3.*

32 Gwagwa et al (n 31) 3.

individuals and society as a whole if left unchecked.[33] The lack of transparency and accountability in AI systems can exacerbate these potential negative impacts.[34] As the use of AI technologies increases, there is a growing necessity to ensure there is regulation that is sufficient in affording the right to equality and protection against discrimination for any persons who stand to be marginalised by such digital change.[35]

In discussing ADM and AI, a closer look must be had at the algorithms involved in these processes and the potential that skewed data and biases have to negatively impact the equality of automated decision-making.

1.3 AI risks and challenges

The use of artificial intelligence in data processing comes with certain risks that have the potential to limit the rights of data subjects not to be discriminated against. Automated decision-making presents a challenge in the form of biased or non-representative data.[36] Data training must occur in order to teach an algorithm to perform an assigned task and then continuously improve the success rate of this task.[37] AI based on biased or non-representative data can entrench existing social or economic inequality by recreating the gaps in representation and the biases of the data sets that are used to train the AI.[38]

A lack of transparency and accountability can further intensify this already negative consequence.[39] POPIA sets out a condition of accountability for responsible parties, and in following this provision, there must be a focus on algorithmic accountability.[40] This concept entails an emphasis on the design and implementation of automated systems that use algorithms in an accountable manner so as to lessen the potential harm or negative impacts that ADM can have on data subjects.[41] However, due to the adaptive and complex nature of algorithmic systems, it is difficult to determine precisely how accountability can be established for an algorithm, as most data

33 As above.
34 As above.
35 ALT Advisory, A.I.MPACT, September 2022, accessible at ai.altadvisory.africa (accessed 10 November 2023).
36 Gwagwa et al (n 31) 3.
37 Ndoro, Johnston & Seymour 'Artificial Intelligence uses, benefits and challenges: A study in the Western Cape of South Africa Financial Services Industry' 2020 *SACAIR 2020 Proceedings: AI in information systems, AI for development and social good* 63.
38 Ndoro et al (n 37) 63.
39 As above.
40 Brand 'Algorithmic decision-making and the law' 2020 *JeDEM* 121.
41 Brand (n 40) 121.

subjects cannot understand the black box of codes and computer processes.[42]

The risks of artificial intelligence are also heightened in developing countries, especially those in Africa.[43] Algorithms are trained in developed Global North countries, and the result is that the training data reflects realities significantly different from those in Africa.[44] The absence of African research and development for AI leads to a lack of contextual application, so certain communities are excluded.[45] This process also affects women, and multiple levels of inequality then become an issue for women in developing countries.[46] The skewed algorithms amplify and echo already-existing inequalities. An example of this data bias is evident in ADM in the Financial Services Industry (FSI). Common sectors of the FSI are credit institutions, mortgage bankers and brokers, holdings and trusts, and the securities and insurance sectors.[47] In Africa, 60% of the 400 million people who lack access to digital financial services are women.[48] 35 million women in Sub-Saharan Africa are excluded from financial services, and the lack of female ownership of a bank account then leads to the data invisibility of African women.[49] With such a large amount of women being absent from data collection in this industry, their personal information cannot be used to train algorithms, and this consequently results in their exclusion from the FSI — among other industries, like housing, social subsidies and other safety nets.[50]

The use of AI algorithms in decision-making thus comes with the risk of perpetuating inequality because if the AI is established in biased or non-representative data, the AI system will reproduce the biases and gaps in the data with which it was trained.[51] Data subjects have the right to equality and, consequently — especially in the context of the dangers of profiling — should be afforded the right to be protected against automated decision-making that has the intention to profile.

2 What is POPIA?

POPIA's aim is to ensure that the processing of all personal information by a responsible party obeys the conditions set out for

42 As above.
43 Gwagwa et al (n 31) 3.
44 Gwagwa et al (n 31) 7.
45 Gwagwa et al (n 31) 4.
46 Gwagwa et al (n 31) 7.
47 Ndoro et al (n 37) 61.
48 Gwagwa et al (n 31) 8.
49 As above.
50 As above.
51 Gwagwa et al (n 31) 4.

lawful processing.[52] The Act is intended to promote the constitutional right to privacy, while protecting the flow of information and access to information.[53] POPIA sets out rules and governs practices for the processing of information, grants individual rights concerning information, and creates an independent regulatory body — the Information Regulator — to enforce these rules and procedures.[54]

2.1 Scope of application

POPIA applies to all processing of personal information which is recorded by a responsible party domiciled in South Africa or one who makes use of automated or non-automated means in South Africa — except if these means are merely used to forward information through South Africa.[55] A 'responsible party' is a private or public body or any other body which, alone or with others, determines the purpose of and means for processing of personal information.[56] A 'data subject' is a person to whom the personal information relates.[57]

'Processing' means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:[58]

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

'Personal information' under POPIA encompasses information which relates to gender, race, marital status, sex and health; information on a financial, medical, educational or criminal history of a person; identifying numbers or symbols, addresses, biometric data, and more.[59] It is information that relates to an individual that he or she does not want to be disclosed to third parties.[60]

POPIA applies to the processing of personal information that is:[61]

52 Burns & Burger-Smidt *Protection of personal information: Law and practice* (2021) 37.
53 Werksmans Attorneys 'Unlocking the why, the how & the who of POPIA' https://www.werksmans.com/wp-content/uploads/2018/11/popia.pdf (accessed 10 November 2023).
54 As above.
55 Burns & Burger-Smidt (n 52) 78.
56 S 1 POPIA.
57 Burns & Burger-Smidt (n 52) 43.
58 S1 POPIA.
59 Burns & Burger-Smidt (n 52) 55.
60 As above.
61 S 3(1) POPIA.

(a) entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and
(b) where the responsible party is—
    (i) domiciled in the Republic; or
    (ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

'Automated means' is any equipment capable of operating automatically in response to given instructions for the purpose of processing information, such as an algorithm.[62] Profiling and the use of Big Data to convey personal information are linked closely with automated decision-making. The use of automated procedures could result in decisions with legal consequences or ones which could affect data subjects to a substantial degree.[63] As seen above, processing can be automated or non-automated.

Sections 6(1)(a)-(e) set down exclusions to the scope of application. POPIA does not apply to the processing of personal information:[64]

(a) in the course of a purely personal or household activity;
(b) that has been de-identified to the extent that it cannot be re-identified again;
(c) by or on behalf of a public body:
    (i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, 134 defence or public safety; or
    (ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities, and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;
(d) by the Cabinet and its committees or the Executive Council of a province; or
(e) relating to the judicial functions of a court referred to in section 166 of the Constitution.

Further statutory exclusions are seen in section 7, which provides an exemption for journalistic, literary or artistic purposes.[65]

62 S 3(1) POPIA.
63 Burns & Burger-Smidt (n 52) 396.
64 S 6(1)(a)-(e) POPIA.
65 S 7 POPIA.

2.2 General principles of processing personal information under POPIA

Chapter 3 of POPIA contains eight conditions for the processing of personal information. These conditions must be observed by responsible parties when personal data is processed. These principles apply to all processing, except where the Act excludes this.[66] Processing is any form of operation, by automated means or not, that concerns the personal information of data subjects.[67] If the processing is automated, it must comply with the eight conditions set out in POPIA.

Below, an overview of the conditions for data processing will explain what is set out in each section.

2.3 The conditions of POPIA explained

Section 8 of POPIA states that:[68]

> The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Essentially, this first principle requires that the responsible party ensures that the conditions set out in Chapter 3 of POPIA are complied with — at all stages and times.[69]

This compliance must be adhered to from the beginning stage of determining the purpose of the processing to processing the data, and finally, to storing the data.[70] The accountability extends further — the responsible party is also liable for the integrity, safety and security of the personal information in their possession or under their control.[71] Importantly, this condition sets out that *all* conditions of Chapter 3 must be complied with throughout the various stages of data processing, each time processing is completed by a responsible party.[72] It is not enough for only some, or even most, of the principles to be complied with.

The second condition places emphasis on the fact that, in order for processing to be lawful, there should be a limit to the reasons why personal information is processed, as well as the type of personal information processed and the subjects from whom this information

66 Burns & Burger-Smidt (n 52) 183-184.
67 Burns & Burger-Smidt (n 52) 396.
68 S 8 POPIA.
69 Burns & Burger-Smidt (n 52) 189.
70 As above.
71 Burns & Burger-Smidt (n 52) 190.
72 As above.

is collected.[73] A limitation on processing is achieved by requiring compliance with the lawfulness and reasonableness of processing; minimality; consent, justification, and objections; and the direct collection of data from the data subject.[74]

Responsible parties must consider why information is required and what type or how much information is necessary for the processing's purpose.[75] According to this condition, only the minimum but adequate amount of information that is relevant may be processed, any information that is seen as excessive or irrelevant could be viewed as unlawful processing.[76]

The third condition relates to purpose specification. Section 13 calls for personal information to be collected only for a specific, explicit, and lawful purpose that is related to the function of the responsible party, and the responsible party must take steps to ensure that the data subject in question has knowledge of the purpose of the data collection.[77]

Section 14 provides that the records of a data subject's personal information must not be kept any longer than is necessary for achieving the original purpose for the collection of this information — unless retention of this information is required by law; the responsible party has a reasonable requirement for accessing the information and this access is lawful and related to its functions or activities; the retention is necessary as a result of a contract between the involved parties; or the data subject has consented to retention of the information.[78]

Next is the fourth condition, which limits further processing of information. This condition states that the responsible party must not stray from the original intention of the processing and may not add additional or alternate purposes for the processing unless such new purpose can be accommodated within the sphere of the initial purpose.[79] This condition therefore ensures the processing of data remains compatible with the original purpose of the collection.[80]

The fifth condition of POPIA sets out an obligation on the responsible party to take reasonable steps to ensure that the personal information held is complete, accurate, updated, and not misleading.[81] A responsible party is therefore, required to verify

73 Snail ka Mtuze & Papadopoulos (n 19) 356.
74 S 9-12 POPIA.
75 S 9-12 POPIA.
76 S 9-12 POPIA.
77 S 13 POPIA.
78 S 14(1)(a)–(d) POPIA.
79 S 15 POPIA.
80 Snail ka Mtuze & Papadopoulos (n 19) 360.
81 S 16 POPIA.

information, use reliable sources and keep information in a way so that it is not ambiguous.[82]

Sections 17 and 18 make up the sixth condition of openness. There are two legs to this condition — namely, maintaining the quality of the personal information and the documentation of the processing, and notification to the data subject during the collection of personal information.[83] Data subjects have a right to know what personal information of theirs is collected or processed by a responsible party, and how this processing is carried out.[84] Accordingly, the legislature has incorporated the values of openness and transparency into POPIA. It is clear that this condition is an incredibly important one, as the knowledge of processing allows the data subject to ensure that their rights are free from infringement.

A data subject must be informed when their personal data is collected.[85] If the personal information is collected directly from the data subject, then they must be informed of the required information before it is collected.[86] In any other case, a data subject must be made aware of the required information before it is collected or as soon as reasonably practicable after collection.[87]

The seventh condition spans sections 19 to 22 of POPIA and governs security safeguards regarding integrity and confidentiality of personal information, as well as operator-processed information and notification of any security compromises.[88] This condition aims to prevent data breaches by ensuring adequate security safeguards are put in place.[89]

The final condition for the lawful processing of data deals with the lawful access of personal information by the data subject, correction of personal information, and method of access.[90] This condition aims to allow data subjects a measure of control and influence over their personal information.[91]

82 Snail ka Mtuze & Papadopoulos (n 19) 361.
83 Burns & Burger-Smidt (n 52) 262.
84 Burns & Burger-Smidt (n 52) 263.
85 Snail ka Mtuze & Papadopoulos (n 19) 361.
86 As above.
87 As above.
88 Burns & Burger-Smidt (n 52) 272.
89 Snail ka Mtuze & Papadopoulos (n 19) 362.
90 Burns & Burger-Smidt (n 52) 280.
91 As above.

2.4 Automated processing and profiling

2.4.1 Overview

Section 71(1) of POPIA gives data subjects the right not to be subject to a decision which could result in legal consequences for that data subject or which affects them to a substantial degree, if that decision is based exclusively on the automated processing of personal information which has the intent of profiling that data subject.[92] The personal information protected against ADM includes a subject's performance at work, credit worthiness, reliability, location, health, personal preferences or conduct.[93]

Profiling is the automated processing of personal information to analyse various aspects of a person's behaviour, personality, and habits in order to make predictions about that person.[94] Automated decision-making can overlap with profiling. Various sources are combined to create a profile of a data subject, who is then treated in accordance with this profile.[95] The types of personal data that are collected for profiling incorporate many aspects of a person's day-to-day life, including categories like health and economic situation.[96] It can be seen that profiling has three elements: it implies an automated form of processing data; it is carried out on personal data; and its purpose is to evaluate personal aspects of a subject in order to predict behaviour and make a decision.[97]

2.4.2 Regulation of ADM and its implications for privacy and data protection

Section 71(2) is an important and tricky piece of legislation. This subsection of POPIA contains a proviso to section 71(1), namely, that ADM of a data subject that has legal consequences *will* be allowed in certain, listed instances.[98] Section 71(1) will not apply if the decision has been 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.[99]

As can be seen from the above discussion, POPIA puts a great deal of emphasis on the values of transparency and accountability.

92 S 71(1) POPIA.
93 S 71(1) POPIA.
94 Roos (n 14) 431.
95 Roos (n 14) 515.
96 Burns & Burger-Smidt (n 52) 418.
97 Burns & Burger-Smidt (n 52) 422.
98 S 71(2) POPIA.
99 S 71(2) POPIA.

However, a question arises as to how effectively the legislature has placed data subjects in a position to exercise their right not to be subject to ADM. I put forth the argument that, in order for a data subject to be able to exercise such a right, it is necessary for the data subject to first be aware that they have been subjected to ADM. To investigate this matter, it must be determined if POPIA provides an express duty of notification to data subjects when automated decision-making takes place.

2.4.3 Right to notification — Section 71

Do either of the two exceptions in section 71(2) provide for a duty of notification to data subjects in the event of automated decision-making? Both subsections specify that 'appropriate measures' must be taken or specified. In section 71(2)(a), POPIA states that the prohibition against ADM will not be applicable if the decision has been taken in connection with the conclusion or execution of a contract when there are 'appropriate measures' established to protect the data subject. Subsection three usefully sets out exactly what these appropriate measures entail. The data subject must be provided with the chance to make representations about the decision, and the responsible party must additionally provide the data subject with enough information about the underlying logic of the automated processing so that the data subject is able to make such a representation.[100]

After careful scrutiny of this section of the legislation, it is evident that there is no duty on the responsible party to notify the data subject of the ADM. The responsible party is, at most, required to present the opportunity for the data subject to make representations — with sufficient knowledge of the logic of the processing involved. This section does not require that the responsible party initially provide the data subject with any notification that they may be entitled to make representations. No duty of notification is found in section 71(2)(a).

Section 71(2)(b) also makes reference to 'appropriate circumstances', although this meaning is much broader than in the preceding subsection. In terms of this section, the prohibition against ADM will not apply if the decision is regulated by a law or a code of conduct in which 'appropriate measures' are specified for protecting the legitimate interests of data subjects.[101] There is not, however, additional guidance on what these appropriate measures constitute. This part of the Act leads to Chapter 7 of POPIA, which sets out the rules and regulations of codes of conduct pertaining to the Act.

100 S 71(3) POPIA.
101 S 71(2)(b) POPIA.

Section 60(4) deals with the need for a code of conduct to specify appropriate measures —

> (ii) for protecting the legitimate interests of data subjects insofar as automated decision-making, as referred to in section 71, is concerned…

At this point, the reader is referred back to section 71, and so a back-and-forth cross-reference begins, with no actual suggestion for the meaning of 'appropriate measures'. At this time, it does not seem that any code of conduct which has been approved or published by the Information Regulator contains confirmation or suggestion of what the appropriate measures of section 71(2)(b) should mean. What is apparent, though, is the fact that there is no explicit duty of notification that requires a responsible party to inform a data subject of automated decision-making. It is clear that neither section 71(2)(a) or (b) provides for an express duty of notification concerning ADM, but perhaps such a duty can be found in another provision of the Act.

2.4.4 Right to notification — Section 18

The openness condition for lawful processing — as discussed above — encompasses the duties of notification of a responsible party. There are various required instances in which the responsible party must take 'reasonably practicable' steps to ensure that the data subject is aware that their personal data is being collected.[102] The openness condition in section 18 deals with the processing of data that occurs at an early stage in the process, namely, the collection of personal information.[103] So, there exists a duty to inform data subjects that their data is being collected. But what of a duty to notify these data subjects when the processing of such data results in a decision or when their personal information is processed automatically?

It seems that the section 18 duty of notification does not extend past the phase in which the data subject's personal information is collected, or reasonably soon after that. This provision POPIA is not intended to give notification after a decision has been made, nor for an instance when personal data is automatically processed any way other than by collection. In light of this, section 18 also lacks a duty of notification regarding automated decision-making.

102 S 18 POPIA.
103 S 18 POPIA.

3 The European Union's General Data Protection Regulation

After analysing the way in which POPIA regulates data protection, it can be seen that section 71 of the Act is insufficient in adequately allowing data subjects to exercise their right not to be subject to automated decision-making under certain circumstances, and it can be argued that the conditions of openness and accountability are not met due to this. These conditions must be met for lawful processing to take place.

POPIA must be compared with its European counterpart, the General Data Protection Regulation (GDPR), to analyse how profiling and ADM fare among each legislation's core values. The foundational concepts of each legislation will be examined to determine if there are any best practices to be utilised by POPIA regarding automated decision-making.

The GDPR came into effect in 2018.[104] The GDPR establishes a baseline of standards for the handling of data for citizens of the European Union in order to protect the processing of personal data.[105] The GDPR has been described as 'the most consequential regulatory development in information policy in a generation',[106] and has become the international benchmark for data protection legislation.[107] It is seen as the gold standard for data protection legislation,[108] which makes it the ideal instrument to compare to the values and policies of POPIA.

3.1 Scope of application

The GDPR aims to protect the fundamental rights of natural persons while their data is processed — without limiting the free movement of personal data within the European Union.[109] The Regulation applies to data processing of personal data by a controller or processor which is established in the EU, regardless of whether the processing occurs within the EU or not.[110] The GDPR additionally applies to the processing of personal data of data subjects who are situated in the

104 Warikandwa 'Personal data security in South Africa's financial services market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation compared' 2021 *PER/PELJ* 14.
105 Warikandwa (n 103) 15.
106 Roos (n 14) 412.
107 Roos 'Data Protection Principles under the GDPR and the POPI Act: A comparison' 2023 *THRHR* 4.
108 Corporate Governance Institute 'GDPR: A gold standard for Europe and beyond' https://www.thecorporategovernanceinstitute.com/webinar/gdpr-a-gold-standard-for-europe-and-beyond/ (accessed 10 November 2023).
109 Roos (n 14) 412.
110 Art 3(1) GDPR.

EU, by a controller or processor not established in the EU, where the processing activities are related to:[111]

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Materially, the GDPR applies to the processing of personal data of data subjects by automated or non-automated means.[112] No distinction is made between processing in the private or public spheres, nor is any distinction made between the different stages of processing (such as collection, recording, storage, use, disclosure, etc.).[113] The GDPR only protects natural and not juristic persons.[114] The GDPR does not apply to processing of personal data for household or purely personal activities,[115] nor does it apply to processing that is done in the course of an activity that falls outside the scope of EU law — matters concerning national security or European security policies, for example.[116] The GDPR additionally does not apply to data processing by authorities for prevention, investigation, detection or prosecution of criminal offences.[117]

3.2 General principles of processing personal information under the GDPR

Similar to POPIA, the GDPR sets out numerous governing principles for the processing of personal information. Article 5 sets out six principles that relate to the processing of personal data:[118]

(1) Personal data shall be:
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

111 Art 3(2) GDPR.
112 Roos (n 14) 413.
113 Roos (n 14) 414.
114 Art 1(1) GDPR.
115 Art 2(2)(c) GDPR.
116 Art 2(2)(d) GDPR.
117 Art 2(2)(d) GDPR.
118 Art 5 GDPR.

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 5(2) sets out the accountability principle — the data controller will be responsible for and able to demonstrate compliance with paragraph 1.

According to the first condition of the GDPR, the processing of personal data should be done lawfully, fairly and in a transparent manner. To be lawful, processing must be based on legitimate grounds, and it must comply with the law.[119] The controller must decide beforehand on a lawful ground for the processing, and the data subject must be notified of any change in the lawful basis for processing.[120]

Fairness under this condition relates to proportionality under European law, and is relevant when interests must be balanced.[121] The principle of transparency requires that data subjects be made aware that their personal data is to be processed.[122] notification must be given regarding the purposes for which the processing is occurring, the identity of the controller or processor, and the rights of the data subject, namely, the right of a data subject to obtain confirmation and communication of their personal data.[123]

The second condition is the purpose limitation. In line with this condition, personal data may only be collected for an explicitly

119 Art 6(1) GDPR.
120 Roos (n 14) 415.
121 As above.
122 As above.
123 As above.

defined purpose.[124] This specific purpose must also be legitimate.[125] Data may not be processed further for purposes which are incompatible with the original specified purpose for the processing.[126]

The third condition sets out that data of a personal nature may only be processed if it is 'adequate, relevant and limited' to what is necessary for the purposes of the processing.[127] This condition sets a standard regarding the quantity of the data that is processed, and the GDPR accountability principle necessitates that a data controller be capable of demonstrating which processes are employed to meet this standard.[128]

The GDPR's fourth condition stipulates that personal data must be accurate and kept up to date, if necessary.[129] If personal data is inaccurate, reasonable steps must be taken to rectify or erase the data.[130] Much like the previous condition, a standard is set (although here, it is one regarding the data quality), and the data controller must be able to show how this standard is adhered to.[131] Only reliable sources must be accepted for processing, and steps must be taken to verify information before the processing happens.[132]

The fifth processing condition requires that personal data be kept in a form which allows for the identification of data subjects for no longer than is necessary for the purpose of processing.[133] To meet this requirement, a controller is expected to set time limits for the erasing of the data or for a review of the data.[134]

In terms of the sixth condition, personal data must be processed in a way that ensures proper and necessary data security.[135] Security measures must be put in place to safeguard an appropriate level of security to prevent risks.[136]

In line with the seventh condition, a data controller is responsible for ensuring compliance with data privacy principles.[137] The controller must be capable of showing compliance with these principles and how effective this compliance is.[138]

124 Roos (n 14) 416.
125 As above.
126 As above.
127 Art 5(1)(c) GDPR.
128 Art 5(1)(c) GDPR.
129 Roos (n 14) 416.
130 As above.
131 Roos (n 14) 417.
132 As above.
133 As above.
134 As above.
135 Roos (n 14) 417.
136 As above.
137 Art 5(2) GDPR.
138 Art 5(2) GDPR.

3.3 Automated decision-making under the GDPR

Under the GDPR, a data subject has the right not to be subject to a decision based solely on automated processing — including profiling — that creates legal or other significant effects for that data subject.[139] Three conditions make up this right: firstly, a decision is made that is, secondly, based solely on automated processing, and, thirdly, the decision has legal effects or other significant effects for the data subject.[140]

The exceptions to the right against ADM in the GDPR are set out in Article 22(2). According to this, ADM is allowed if the decision is necessary for the creation or performance of a contract, if the decision is authorised by a law that lays down adequate protective measures, or if the decision is based on a data subject's explicit consent.[141]

3.4 Differences between POPIA and the GDPR

3.4.1 Regulatory strategies

POPIA has adopted the 'command-and-control' mode of regulation that appears in the GDPR, but as will be seen, POPIA has neglected to embrace the collaborative governance features of the GDPR.[142] Collaborative governance regulation, as Bronstein explains, corresponds with the notion of decentred regulation — this incorporates self-regulation and co-regulation.[143] Command-and-control regulation, conversely, is based on the concept of law as the 'command of a sovereign backed by sanctions'.[144] This type of regulatory strategy has been criticised as being ineffectual and not cost-effective — a vast amount of resources must be used to deploy sanctions for this theory to be effective.[145] In a democratic context, this strategy is seen as largely unattainable, especially in South Africa, where efforts for large-scale compliance are usually unreachable.[146] Another positive for the collaborative governance theory is provided in the context of data protection. Bronstein argues that it is impractical for governments to regulate the cyber world, as government regulators will always have to deal with a lack of

139 Art 22(1) GDPR.
140 Roos (n 14) 431-432.
141 Art 22(2) GDPR.
142 Bronstein 'Prioritising command-and-control over collaborative governance: The role of the Information Regulator Under The Protection of Personal Information Act' 2021 *PER/PELJ* 6.
143 Bronstein (n 141) 6.
144 As above.
145 Bronstein (n 141) 7.
146 As above.

information and expertise.[147] It can be seen that, for regulation to be fully effective, there must be multiple mechanisms of accountability, and the collaborative governance strategy is designed to provide this.[148]

3.4.2 Codes of conduct

Another difference between pieces of legislation is seen in how the GDPR and POPIA govern codes of conduct. POPIA, in its command-and-control method, provides that codes of conduct that are issued become binding on responsible parties. Codes of conduct under POPIA are comparable with subordinate legislation — the code is binding on a specific sector regardless of the views of those subject to it.[149] In contrast, codes of conduct set out in the GDPR are considered voluntary for data controllers.[150] The GDPR intends for codes of conduct to fulfil a normative function that accelerates compliance.[151] This strategy is designed to lead to greater adherence to the voluntary rules over time as a result of involving the private sector in its own regulation — a clear collaborative approach by the GDPR.[152]

3.4.3 Remedies for automated decision-making under POPIA and the GDPR

Section 71 of POPIA and Article 22 of the GDPR provide remedies that allow individuals to protect their personal information from automated decision-making that involves profiling. As can be seen by the legislation, the safeguards in this section and article, respectively, are almost identical and prohibit a data subject from being exposed to automated decision-making and profiling.[153] POPIA provides a general remedy against ADM, but the GDPR departs from this by opting to incorporate a requirement that aims to improve, on a systemic level, the quality of ADM that, includes profiling.[154] With this GDPR measure, a potential best practice for POPIA and ADM can be found to improve accountability and openness and better protect data subjects from processing.

147 Bronstein (n 141) 8.
148 Bronstein (n 141) 9.
149 Bronstein (n 141) 17.
150 Bronstein (n 141) 16.
151 As above.
152 Bronstein (n 141) 17.
153 S 71 POPIA; Art 22 GDPR.
154 Bronstein (n 141) 18.

3.4.4 Right to be informed

According to the GDPR, if the processing of personal data involves automated decision-making, then the data subject must be informed of this — as well as the significance of this processing and the expected consequences of the processing.[155]

The right to notification of a data subject was discussed in Chapter 3, and there, it was concluded that neither section 71 nor section 18 of POPIA provides an express duty of notification regarding ADM. Comparatively, the GDPR does expressly dictate that a data controller must inform a data subject about the existence of automated decision-making. I put forth that because of POPIA's lack of a similar duty, no obligation exists for a responsible party to give notice of ADM taking place during the processing. With no such obligation to inform the data subject, this brings about the potential for violation of the data subject's right to be protected against ADM, and the Act does not meet the conditions of accountability and transparency. This is an area that POPIA falls short in, and the Act could adopt the GDPR's express duty as a best practice to better promote the rights of data subjects.

3.4.5 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process whereby data protection risk can be identified and managed.[156] The process starts with the structured assessment of a data processing activity to classify any risks for data protection that exist in the activity.[157] It must then be determined if such risks are legally compliant, and a data controller can consequently take any necessary action to mitigate the identified risks.[158] According to Whitcroft, DPIAs in the EU assist in establishing compliance with data protection standards — especially in accordance with the accountability requirement.[159]

The Article 29 Working Party Guidelines describe a DPIA as:[160]

> … a process for building and demonstrating compliance by systemically examining automated processing techniques to determine the measures necessary to manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

155 Art 13(2)(f) GDPR.
156 Burns & Burger-Smidt (52) 432.
157 As above.
158 As above.
159 Whitcroft 'Data protection impact assessments' in Carey *Data protection: A practical guide to UK law* (2020) 237.
160 Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679.

DPIAs are significant tools for accountability, as they help data controllers comply with the GDPR requirements.[161] A Data Protection Impact Assessment is compulsory when there is a 'high risk' to the rights and freedoms of natural persons.[162] According to the duty set out in Article 35(1) of the GDPR, a data controller must assess the impact of the proposed processing on personal data protection, where such processing is likely to result in high risk to the rights and freedoms of natural persons.

Under POPIA, no reference is made to a risk assessment such as a DPIA. The section regarding assessments in the Act only refers to whether data processing complies with the provisions of POPIA.[163] In addition to this, there is no duty to make such an assessment prior to the processing of personal data.[164] It can, therefore, be seen that there is no similar concept to DPIAs in POPIA.

The use of DPIAs prior to automated data processing would introduce a best practice for POPIA. This process can provide coherence before automated decision-making even begins for a data subject, and the practice would create an additional layer of transparency and accountability for the responsible party — something that should be strived for to meet the conditions for lawful processing set out in the Act.

While both POPIA and the GDPR share aspects of regulation, strengths, and conditions for data protection, there are many best practices of the GDPR that POPIA could adopt to better protect data subjects from ADM. Regulatory strategies, codes of conduct, remedies, explicit notification, and DPIAs are all areas that could be improved POPIA.

4 Conclusion

The regulatory framework of POPIA sets out to protect the privacy of personal information of data subjects, and in many ways, the Act meets its objective. However, there are areas in the legislation that need to be improved for proper data protection. POPIA emphasises the importance of processing in line with the values of transparency and accountability. However, with its lack of express notification to data subjects regarding ADM, it is evident that POPIA could be more effective in allowing data subjects to exercise their right not to be subject to ADM. The data subject can only effectively exercise this right if they are aware of it in the first place. This conflicts with the aims set out in POPIA; the data subject is left without an opportunity

161 Burns & Burger-Smidt (n 52) 432.
162 Art 35(1) GDPR.
163 Burns & Burger-Smidt (n 52) 432.
164 As above.

to exercise and be protected by their right. A solution to this would be for POPIA to implement an explicit obligation of notification on responsible parties. Alternatively, the Information Regulator could publish a code of conduct for section 71(2)(b) of POPIA that specifies 'appropriate measures' for protecting the interests of data subjects concerning ADM. This way, a duty of notification for ADM could be established, and a data subject could rely on section 71 for adequate protection.

POPIA can also improve on its aims of accountability and transparency — as well as better data subject protection — by implementing the best practices found in the GDPR. Most practically, introducing Data Protection Impact Assessments would create more transparency and responsibility for a responsible party. By enforcing a risk assessment to be completed before data processing occurs, the risk of impairing the rights and freedoms of data subjects would be lessened.

POPIA does not sufficiently allow data subjects to exercise their right not to be subject to automated decision-making. The Act has done well in introducing comprehensive data protection legislation, but several areas can be amended to ensure proper protection. Until such a time that new practices are implemented, however, data subjects in South Africa are not entirely safeguarded against the dangers of automated processing, algorithms and AI.