Volume **7** (3) 2025 https://doi.org/10.5204/lthj.4081

Automated Decision-Making and the Right to an Explanation Under POPIA in South Africa: A Legal Perspective

Zinhle Novazi
Stellenbosch University, South Africa

Abstract

The Protection of Personal Information Act 4 of 2013 (POPIA) establishes crucial safeguards against the risks posed by automated decision-making (ADM), particularly under section 71. This section restricts ADM that produces significant legal or personal effects unless specific exceptions apply. However, POPIA does not explicitly grant a right to an explanation, leaving uncertainties around how data subjects can meaningfully contest or understand ADM decisions. Using a doctrinal and comparative methodology, this article examines the legal implications of the provisions of section 71, focusing on its interpretation as either a prohibition against ADM or merely a right to object. The findings highlight the practical and theoretical challenges of defining 'solely automated' processes, revealing potential loopholes where nominal human oversight may undermine protections. Comparisons are drawn with international frameworks, such as the European Union's General Data Protection Regulation (GDPR), to explore how a right to explanation might enhance transparency, accountability, and data subject rights under POPIA. The article further investigates the adequacy of POPIA's 'appropriate measures' requirement, including the necessity of notification rights and clear standards for providing meaningful explanations. By distinguishing between *ex-ante* and *ex-post* explanations and between system functionality versus specific decision rationales, it identifies gaps in POPIA's framework and proposes legal reforms. The article concludes that POPIA requires reform to strengthen algorithmic accountability and data subject protection. It recommends introducing an explicit right to explanation, clarifying the scope of ADM prohibitions, and implementing independent auditing mechanisms to strike a balance between innovation and accountability.

Keywords*:* Data protection; automated decision-making; POPIA; GDPR; right to explanation; South Africa.

1. Introduction

The increasing integration of artificial intelligence (AI) into various sectors has presented both opportunities and challenges, particularly concerning automated decision-making (ADM).[1] ADM systems operate without direct human involvement and are widely used in the banking, employment, and healthcare domains. While these technologies can enhance efficiency and decision-making capabilities, they also raise significant concerns regarding their impact on individuals' fundamental rights.[2] As a result, governments, institutions, and human rights organisations are actively working toward regulatory frameworks that ensure these systems are transparent, accountable, and aligned with societal values.[3]

A central debate surrounding ADM regulation is whether individuals subjected to algorithmic decisions should have a legally enforceable right to an explanation of the decision-making process.[4] In jurisdictions like the European Union (EU), the General

[1] Remolina, Role of Financial Regulators, 1–14.
[2] Singh, "Social Sorting as 'Social Transformation'," 365–383.
[3] Temme, "Algorithms and Transparency," 475–477.
[4] Dimitrova, "The Right to Explanation," 211–218.

Data Protection Regulation (GDPR)[5] has introduced provisions requiring data controllers to provide meaningful information about the logic, significance, and consequences of ADM processes.[6] However, legal scholars continue to debate whether these provisions amount to a formal right to explanation or merely require some level of transparency.[7] Similar discussions are emerging in South Africa regarding the adequacy of existing legal protections under the *Protection of Personal Information Act 4 of 2013* (POPIA), particularly section 71, which restricts ADM that significantly affects data subjects.

The relevance of this discussion is particularly pronounced in South Africa, a country marked by deep-rooted socio-economic inequalities.[8] South Africa remains one of the most unequal societies in the world, with extreme disparities in income and wealth distribution.[9] Beyond economic inequality, systemic barriers to market access, the influence of macroeconomic policies, and environmental disparities further entrench these divisions.[10] Given this historical context, the potential for ADM systems to reinforce or exacerbate existing biases presents a serious concern. If left unchecked, AI-driven decisions could replicate historical patterns of exclusion and discrimination, particularly in sectors such as credit scoring, hiring, and social welfare allocation.[11] Scholars such as Adewoyin and Sampene have already found that AI biases are inherently problematic in ADM, while cases in which courts have frowned upon unexplainable AI decisions that negatively affect data subjects without providing room for analysing how the decisions were arrived at. AI can therefore no longer be the sole arbiter in complex human problems.[12]

The lack of an explicit right to an explanation in POPIA raises critical questions about the extent to which individuals can contest or understand algorithmic decisions that significantly impact their lives.[13] Transparency in ADM is essential to ensuring accountability, detecting algorithmic bias, and enabling meaningful challenges to unfair outcomes.[14] Without clear legal mandates requiring explanations, individuals may struggle to understand the rationale behind automated decisions, thereby limiting their ability to exercise their rights effectively.[15] This is particularly concerning in a country like South Africa, where historical injustices necessitate stronger legal safeguards to prevent the perpetuation of discrimination through AI-driven processes.[16]

This article examines the legal implications of ADM under POPIA, focusing particularly on the interpretation of section 71 as either a prohibition against ADM or merely a right to object. It investigates whether South Africa's current regulatory framework offers adequate protection for data subjects or if further legal reforms, such as establishing an explicit right to explanation, are needed to improve transparency and fairness. By comparing POPIA with international frameworks such as the GDPR, this study emphasises the importance of strong ADM safeguards in promoting trust, accountability, and fair digital governance.

Ultimately, the article argues that South Africa must consider strengthening its data protection legal framework to ensure that ADM does not exacerbate existing inequalities. The introduction of clear requirements for algorithmic transparency, combined with external auditing mechanisms, could help strike a balance between innovation and the protection of fundamental rights. By doing so, South Africa would take an important step toward promoting fairness and inclusivity in the digital age.

2. What is ADM in Terms of Section 71, and why is the Right to an Explanation Important?

Considering the extensive use of personal data in AI applications and the specific data protection rules regarding explainability and accountability of automated decisions, POPIA in South Africa appears to be one of the most advanced, robust, and

[5] European Parliament and Court of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),* [2016] OJ L 119/1, as corrected by Corrigendum, [2018] OJ L 127/2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.
[6] *General Data Protection Regulation (GDPR),* arts. 13, 14, 15, and 22, Recital 71.
[7] Goodman, "European Union Regulations," 27-28.
[8] Francis, "Poverty and Inequality in South Africa," 788–789.
[9] Orthofer, "Wealth Inequality in South Africa," 1–5.
[10] Singh, "Social Sorting as 'Social Transformation'" 365.
[11] Kleinberg, "Discrimination in the Age of Algorithms," 124–144.
[12] Adewoyin, "Artificial Intelligence and Sustainable Energy Development," 196–203; Sampene, "Artificial Intelligence as a Pathway to Africa's Transformations," 14939–14951.
[13] Temme, "Algorithms and Transparency," 473–474.
[14] Temme, "Algorithms and Transparency," 473–474.
[15] Dimitrova, "The Right to Explanation," 211–218.
[16] Francis, "Poverty and Inequality in South Africa," 788–789.

comprehensive legal tools for regulating personal data in AI.[17] One of its primary objectives is to protect fundamental human rights, particularly when individuals are subject to profiling and ADM.[18]

In Chapter 3, POPIA establishes crucial conditions for processing personal information, including accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation.[19] These conditions are essential for ensuring trustworthy AI applications. However, the right to an explanation also finds constitutional grounding in the interplay between the right to privacy and the right of access to information, both entrenched in the Bill of Rights. Sections 14 and 32 of the *Constitution of the Republic of South Africa, 1996* (Constitution) bind both natural and juristic persons, reflecting the horizontal application of these rights. The right to privacy protects individuals' personal sphere and gives them control over information about themselves, including data held by others.[20] Conversely, section 32(1)(b) of the Constitution grants everyone the right to access information held by another person when that information is required for the exercise or protection of a right.[21] This balance between the two rights illustrates that privacy is not absolute, and it may be limited.

Although both the Constitution and POPIA recognise rights of 'access to information,' they serve distinct yet complementary functions. The constitutional right of access to information in section 32 of the Constitution is given effect through the *Promotion of Access to Information Act 2 of 2000* (PAIA) and is fundamentally oriented towards transparency.[22] It enables any person to obtain records held by the state or by another person when such information is required for the exercise or protection of a right. In contrast, section 23 of POPIA confers a privacy-oriented right of access: it allows a data subject to request confirmation of whether a responsible party holds personal information about them, and to obtain a description, record, or copy of such information.[23] In practical terms, PAIA is used to gain access to information while POPIA is used to protect and manage personal information.

Section 71 provides data subjects with the right not to be subject to decisions based solely on automated processing that results in legal consequences or significantly affects them.[24] However, there are specific exceptions to this prohibition. A decision may be based on automated processing if it:

- has been taken in connection with the conclusion or execution of a contract, and the request of the data subject in terms of the contract has been met;[25] or
- appropriate measures have been taken to protect the data subject's legitimate interests;[26] or
- it is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.[27]

Beyond these exceptions, section 71(3), alongside sections 16, 17, and 18 of POPIA, requires that data subjects be informed about the existence of ADM processes, the underlying mechanisms (logic) of such processes, and the significance and potential consequences of these decisions.[28] These provisions align with the broader principles of transparency and accountability in AI regulation.

Different levels of explanation can be identified in ADM. A general explanation provides insight into the overall logic of an AI system, while more granular explanations detail how an AI application functions in specific situations or even in individual cases.[29] These explanations are vital for enabling data subjects to contest algorithmic outputs and assert their right to human

[17] The preamble of POPIA states that it seeks to safeguard personal information handled by both public and private entities. It achieves this by setting specific conditions for lawful data processing.
[18] As above.
[19] Townsend, "Navigating Uncharted Waters," 342.
[20] *Bernstein v Bester NO*, 1996 (2) SA 751 (CC), para 76. In *Investigating Directorate v Hyundai Motor Distributors; In re: Hyundai Motor Distributors v Smit NO*, 2001 (1) SA 545 (CC), para 18.
[21] See *Arena Holdings (Pty) Ltd t/a Financial Mail v South African Revenue Services*, 2022 (2) SA 485 (GP), para 10.3.
[22] See *Brümmer v Minister for Social Development*, 2009 (6) SA 323 (CC), para 63.
[23] *Tiso Blackstar Group (Pty) Ltd v Steinhoff International Holdings N.V.*, 2023 (1) SA 283 (WCC), paras 58–63.
[24] POPIA, sec. 71.
[25] POPIA, sec. 71(2)(a).
[26] POPIA, sec. 71(2)(a)(ii).
[27] POPIA, sec. 71(2)(b).
[28] Wachter, "Why a Right to Explanation," 77–85.
[29] Selbst, "Intuitive Appeal," 1107.

intervention.[30] Furthermore, sections 16 (data quality), 17 (processing documentation), and 18 (data subject notification) of POPIA play a role in ensuring that data subjects are provided with meaningful insights into ADM processes.

The right to an explanation is increasingly seen as a critical mechanism for ensuring accountability and transparency in algorithms, AI, robotics, and other automated systems.[31] ADM systems can produce unintended and unexpected results, which can be difficult to assess due to the complexity and opacity of algorithmic mechanisms.[32] The right to an explanation would require data controllers to clarify how these mechanisms reach their decisions, making it easier for individuals to understand and challenge such outcomes.

POPIA does not explicitly provide a right to an explanation in the same manner as the GDPR provides a right to explanation in its recitals.[33] However, legal scholars have proposed two interpretative approaches to infer such a right from various provisions.[34] The first approach relies on the safeguards required under section 71(3) and related provisions in sections 15, 17, and 18 to establish a right to explanation. The second approach emphasises the obligation of the responsible party to provide a data subject with sufficient information about the logic behind automated processing to enable them to make informed representations.[35]

The right to an explanation serves as a cornerstone for safeguarding against the risks of ADM. Ideally, responsible parties should disclose key details, including the categories of data used, the relevance of these categories, the statistical models applied in profiling, how profiles influence decision-making, and how they impact individual data subjects.[36] Profiling through ADM can potentially lead to unfair treatment and discrimination, denying individuals access to employment, credit, or insurance opportunities.[37] Ensuring that ADM processes are transparent and explainable is, therefore, essential in mitigating these risks and upholding data protection principles under POPIA.

2.1 The Limitations of Section 71: Interpreting 'Solely Automated' Decisions and the Need for a Right to Explanation

Section 71 of POPIA is designed to protect data subjects from the potential risks associated with decisions made solely through automated processing. However, its applicability is constrained by its wording, particularly in its reference to decisions 'based solely on the basis of automated processing of personal information.[38] This limitation raises interpretative challenges and creates potential loopholes in its enforcement, particularly regarding the extent of human involvement necessary to remove a decision from the scope of the provision.[39]

Section 5(1)(g) of POPIA establishes that a data subject has the right 'not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71.' While this provision aims to safeguard individuals against fully ADM, its effectiveness is limited by its restrictive scope. The provision applies exclusively to decisions that are "based solely on the basis of automated processing of personal information", excluding instances where minimal human intervention occurs.[40] This wording presents a significant limitation, as it does not account for cases where a human merely rubber-stamps an automated decision, thereby circumventing the intended purpose of the protection.[41]

[30] Wachter, "Why a Right to Explanation," 77–85.
[31] Edwards, "Enslaving the Algorithm," 50–54.
[32] Rudin, "Stop Explaining Black Box," 206–215.
[33] *General Data Protection Regulation (GDPR)*, arts. 13, 14, 15, 22 and Recital 71.
[34] Dimitrova, "The Right to Explanation," 211–218.
[35] Edwards, "Enslaving the Algorithm," 50–54.
[36] Information Commissioner's Office, "Rights Related to Automated Decision Making."
[37] Wiedemann, "Profiling and (Automated) Decision-Making," 3–4. See also *General Data Protection Regulation (GDPR),* art. 4(4) that defines profiling as 'any form of automated processing of personal data … to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.'
[38] POPIA, sec. 71.
[39] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21.
[40] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21. According to Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, human involvement should be meaningful, and it should be carried out by someone who has authority and competence to change the decision.
[41] Mendoza, "The Right Not to Be Subject," 87. See also Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21, which states: 'To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than a token gesture.'

The strict interpretation of 'based solely on the basis of automated processing' raises concerns about the potential for tokenistic human intervention to bypass the restrictions of section 71.[42] While this article acknowledges that a broader interpretive frame that considers the policy and interest objectives underlying POPIA could potentially illuminate the legislator's intent and close the interpretive gaps, the analysis proceeds from a legal rather than a policy perspective. It employs a doctrinal and comparative approach to interpret and assess section 71 within its legal context. A comparison with international legal frameworks, particularly the GDPR, illustrates similar challenges. A key example is the German *Schufa* case,[43] which questioned whether using automated processes to prepare a decision, where a human merely approves or accepts the automated outcome, qualifies as exclusively ADM.[44] This case highlights the ambiguity in determining whether human involvement, however minimal, removes a decision from the category of 'solely automated' processing.[45]

Legal scholars have identified the risk of 'quasi-automation,' in which a decision-making process remains functionally automated, yet a human figure is inserted at the end to lend the appearance of oversight.[46] Wagner has argued that such superficial human involvement serves as a basic rubber-stamping mechanism in an otherwise entirely automated system.[47] The consequence of this interpretative loophole is that organisations can introduce nominal human oversight to evade compliance with section 71, thereby undermining its protective function.

The European Data Protection Board (EDPB) has sought to clarify the requirements for meaningful human oversight in the context of ADM under the GDPR.[48] According to its guidelines, human involvement must be 'meaningful' rather than a mere token presence.[49] This means that the human reviewer must possess both the authority and competence to alter the decision, rather than merely approving an algorithmic output without scrutiny.[50] The requirement of meaningful intervention ensures that the role of a human in decision-making extends beyond formality and incorporates genuine critical evaluation of the automated outcome.[51]

Without such safeguards, there is a risk that humans will serve as scapegoats for AI-based decision-making. Scholars such as Green,[52] have argued that oversight mechanisms often fail to correct biases or errors in automated decisions, as human reviewers may lack the expertise, time, or incentive to challenge algorithmic recommendations.[53] Consequently, humans may simply bear the legal and ethical responsibility for flawed decisions without exercising substantive control.

The limitations of section 71 highlight the need for stronger transparency measures, including a right to explanation.[54] Even if a human ultimately makes the decision based on an algorithmically-generated score, this does not diminish the data subject's legitimate interest in understanding how the algorithm arrived at its recommendation.[55] The GDPR does not explicitly define what constitutes 'solely automated' decision-making, which has led to concerns that token human involvement may be used to bypass the protections of Article 22. Similarly, POPIA's lack of clarity on this issue raises concerns that organisations may exploit the 'solely automated' loophole to justify high-stakes AI-based decision-making without genuine oversight.[56]

A right to explanation would ensure that data subjects receive sufficient information about how decisions affecting them have been made, even when some human intervention occurs.[57] This would require responsible parties to disclose the categories of data used, the statistical models applied, and the relevance of profiling to the decision-making process.[58] Such disclosures are

[42] Mendoza, "The Right Not to Be Subject," 87–88.
[43] Case C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957 (CJEU, December 7, 2023); Opinion of Advocate General Pikamäe in *SCHUFA Holding*, ECLI:EU:C:2023:220 (CJEU, March 16, 2023).
[44] Silveira, "Automated Individual Decision-Making," 75.
[45] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21.
[46] Wagner, "Liable, but Not in Control?," 114–120.
[47] Wagner, "Efficiency vs. Accountability?," 12.
[48] POPIA, sec. 71 only applies only if there is no human involvement in the decision process and similarly in the case of *General Data Protection Regulation (GDPR),* art. 22. See also Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 20–21.
[49] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 20–21.
[50] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 20–21.
[51] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 20–21.
[52] Green, "The Flaws of Policies," 5.
[53] Green, "The Flaws of Policies," 5.
[54] Naudts, "Meaningful Transparency," 531–540.
[55] Green, "The Flaws of Policies," 5.
[56] POPIA, sec. 71(1).
[57] Metikoš, "The Right to an Explanation," 17–24.
[58] Metikoš, "The Right to an Explanation," 17–24.

essential to prevent unfair discrimination, particularly in contexts such as employment, credit scoring, and insurance, where profiling can have profound and potentially adverse consequences.[59]

By addressing the interpretative loopholes in section 71 and introducing greater transparency through a right to explanation, South Africa can strengthen its regulatory framework for AI-based decision-making, thereby enhancing accountability and protecting individuals from potentially harmful automated processes.

2.2 What Does 'Affects the Data Subject to a Substantial Degree' Mean?

Section 71(1) of POPIA restricts ADM where such decisions have 'legal consequences' or 'affect the data subject to a substantial degree.'[60] However, the phrase "affects the data subject to a substantial degree" remains ambiguous and lacks precise legal interpretation within the Act. There is currently no South African case law interpreting the phrase 'affects the data subject to a substantial degree' under section 71(1) of POPIA, leaving its scope uncertain. However, this ambiguity could be challenged through judicial interpretation or constitutional review on the grounds of vagueness and inadequate protection of the right to privacy.[61] This section seeks to clarify the meaning and scope of this provision by considering relevant legal perspectives and comparative insights from the GDPR.[62]

The absence of a statutory definition for 'affects the data subject to a substantial degree' raises questions about its scope and applicability.[63] The section provides examples of automated decisions that might fall within its ambit, including those that:

- provide a profile of a person's performance at work;[64]
- assess a person's creditworthiness, reliability, or location;[65]
- relate to health, personal preferences, or conduct.[66]

A key question is whether this list is exhaustive or indicative. If the list is closed, then only the scenarios explicitly mentioned in the provision would qualify as substantially affecting a data subject. If it is illustrative, other types of automated decisions with significant personal consequences may also fall within the scope of section 71(1).[67] The lack of clarity necessitates further interpretation, particularly in light of comparative legal frameworks.

A crucial interpretive issue is whether the assessment of 'substantial degree' is subjective (based on the perspective of the affected individual) or objective (determined by an external standard).[68] This distinction is important, as different individuals may perceive the impact of automated decisions differently. If interpreted subjectively, any decision that a data subject

[59] Kleinberg, "Discrimination in the Age of Algorithms," 124–144. See also Allen, "Artificial Intelligence," 588.
[60] POPIA, sec. 71(1). Similarly, in the EU the scope of regulations on automated decision-making, like art. 22 GDPR and art. 15 of *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement (DPD)*, extends beyond decisions that solely affect a person's legal rights or status to include those that have a similarly significant impact on their lives.
[61] See *Investigating Directorate v Hyundai Motor Distributors; In re: Hyundai Motor Distributors v Smit NO*, 2001 (1) SA 545 (CC), para 21 and the argument of Mokgoro J in *S v Makwanyane*, 1995 (3) SA 391 (CC), para 300.
[62] It could be argued that the inclusion of 'affects the data subject to a substantial degree' indicates that the provision's scope extends beyond decisions that directly affect a person's legal rights or status. It seems that the intention for both the GDPR and POPIA is to protect individuals from automated decisions that have a comparable level of impact on their lives even if those impacts are not legal.
[63] POPIA, sec. 71(1). When compared with art. 22 GDPR, significant effects in terms of Recital 71 of the GDPR is interpreted to include any circumstance that 'significantly influences the circumstances, behaviour or choices' of the data subject. According to the EDPB's interpretation, examples would include 'automatic refusal of an online credit application or e-recruiting practices without any human intervention.'
[64] POPIA, sec. 71(1).
[65] POPIA, sec. 71(1). See also Johnson, "Artificial Intelligence," 506.
[66] POPIA, sec. 71(1).
[67] POPIA, sec. 71(1). It may be worthwhile to examine how this provision has been interpreted in relation to the GDPR recitals to better inform our understanding of its likely interpretation. Recital 71 of the GDPR provides concrete examples, such as the automatic refusal of an online credit application and e-recruiting practices, as instances that might constitute legal or similarly significant effects. This suggests that other scenarios with comparable impacts could also fall under the provision.
[68] It is worth noting that under *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), [2024] OJ L, 2024/1689*, https://eur-lex.europa.eu/eli/reg/2024/1689/oj, art. 86(1) and Recital 171 it is up to the individual themselves to assess whether or not they are significantly affected. While this applies to the Artificial Intelligence Act, the concept of 'significant effects' under the GDPR and POPIA seems to be related.

perceives as having a major impact on their life could be subject to the restrictions in section 71.[69] An objective approach, on the other hand, would likely require a more concrete standard, possibly assessed by regulators or courts.[70]

Comparatively, the GDPR uses the term 'significant effects' rather than 'substantial degree.'[71] The EDPB has clarified that legal effects under the GDPR include consequences that impact an individual's legal rights, such as the right to associate, vote, or take legal action. Significant effects, on the other hand, encompass any circumstance that significantly influences a data subject's behaviour, choices, or circumstances.[72] Examples include automatic refusals of credit applications or recruitment decisions made without human involvement. In the case of *Dun & Bradstreet*,[73] the Court of Justice of the European Union (CJEU) recognised that a credit score generated through automated processing could constitute both a legal and significant impact on an individual.[74]

The EDPB has provided interpretive guidance on decisions that produce 'legal effects' or 'significantly affect' individuals, which may offer insights for understanding section 71 of POPIA.[75] According to the EDPB:

- 'Legal effects' include decisions that impact legal rights, such as the right to vote, freedom of association, or entitlement to social benefits.[76]
- "Significant effects" refer to decisions that influence a data subject's circumstances, behaviour, or choices in a meaningful way.[77] Examples include automatic refusal of credit applications and AI-driven hiring decisions.

Notably, in the *OQ v Land Hessen (Schufa)*,[78] Advocate-General Pikamäe argued that a credit score generated through automated processing constitutes both a legal and significant impact.[79] Applying this reasoning to POPIA, it could be argued that decisions affecting employment opportunities, financial access, or social benefits should fall within the "substantial degree" threshold.[80]If a decision must be "substantial" before triggering the protections of section 71, this may limit the scope of a data subject's rights under POPIA. This requirement implies that minor automated decisions, such as personalised recommendations in online shopping, may not qualify.[81] However, where an automated decision significantly alters an individual's economic or social standing, the right to an explanation should be enforceable. The challenge remains in establishing a clear threshold for what qualifies as "substantial". A broader interpretation would enhance protections for individuals but may impose additional compliance burdens on organisations using AI-driven decision-making.[82] A more restrictive interpretation, however, risks creating loopholes where impactful decisions escape scrutiny.

The phrase "affects the data subject to a substantial degree" within section 71 of POPIA remains open to interpretation. Drawing from the GDPR, the threshold should include decisions that significantly impact legal rights, financial access, and essential life choices.[83] Given the increasing reliance on AI in decision-making, regulatory clarity is necessary to ensure data subjects are adequately protected under POPIA. Future guidance or judicial interpretation will be crucial in defining this standard more precisely.

[69] Miao, "Debating the Right to Explanation," 876–877.
[70] Miao, "Debating the Right to Explanation," 876–877.
[71] *General Data Protection Regulation (GDPR),* art. 22.
[72] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21.
[73] The CJEU held that in case of automated decision-making, an explanation of the procedure and principles actually applied must be provided to the data subject under the *General Data Protection Regulation (GDPR)*, art. 15(1)(h).
[74] Case C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2024:218 (CJEU, March 7, 2024)**.**
[75] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21.
[76] POPIA, sec. 71(1).
[77] *General Data Protection Regulation (GDPR),* Recital 71 provides the following typical examples: 'automatic refusal of an online credit application' or 'e-recruiting practices without any human intervention.'
[78] Case C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957 (CJEU, December 7, 2023) (request for a preliminary ruling from the *Verwaltungsgericht Wiesbaden,* Germany); *OQ v Land Hessen* (Reference for a preliminary ruling).
[79] Opinion of Advocate General Pikamäe in the *Schufa* case. See also Silveira, "Automated Individual Decision-Making," 75.
[80] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21. See also Opinion of Advocate General Pikamäe in *Schufa* paras 36–52. Advocate General Pikamäe argues that even if not strictly 'legal,' a credit score undeniably has a substantial impact on an individual's financial circumstances and their ability to participate in various aspects of modern life, such as renting an apartment, etc.
[81] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21.
[82] See Opinion of Advocate General Pikamäe in the *Schufa* case. Advocate-General Pikamäe's argument in this case, that a credit score has both legal and significant effects, supports a relatively broad interpretation of significant effects.
[83] *General Data Protection Regulation (GDPR)*, art. 22, Recital 22.

2.3 Should Section 71 be Interpreted as a Right to Object or as a Prohibition?

Section 71 of POPIA presents an important legal question regarding whether it should be understood as a right to object to ADM or as a prohibition on such processing unless specific conditions are met. The distinction between these interpretations carries significant consequences for both data subjects and responsible parties.

If section 71 is interpreted as a right to object, ADM is allowed by default unless the data subject actively opposes it.[84] This interpretation places the burden on individuals to be aware of ADM processes affecting them and to take the necessary steps to challenge them.[85] If an objection is raised, the responsible party would then need to justify the decision under section 71(2), which permits ADM in specific circumstances, such as contractual necessity, explicit consent, or authorisation by law.[86] However, if an automated decision falls within these exceptions, the data subject may have limited grounds to challenge it further.

Conversely, if section 71 is read as a prohibition, responsible parties would be barred from making decisions based solely on automated processing unless one of the three conditions in section 71(2) is met.[87] In this scenario, the default position favours greater data protection, ensuring that individuals do not need to take proactive steps to prevent ADM from impacting their rights.[88] This interpretation aligns with the broader transparency and fairness principles underlying data protection laws, including obligations on responsible parties under section 18 of POPIA to notify data subjects when their information is being processed.[89]

The wording of section 71, which states that a data subject "shall have the right not to be subject to" ADM with legal or similarly significant effects, supports both interpretations.[90] On the one hand, the phrase suggests a prohibition unless certain conditions are met, implying that ADM is not permissible unless explicitly justified.[91] On the other hand, it could be read as granting individuals a right to contest such processing, requiring them to take action before restrictions apply.[92]

The practical impact of these interpretations is substantial. If section 71 functions as a prohibition, responsible parties would need to demonstrate compliance with section 71(2) before engaging in ADM.[93] This approach offers stronger safeguards for data subjects by preventing unauthorised processing before it occurs. In contrast, treating section 71 as a right to object means that ADM can proceed unchecked unless an individual actively intervenes.[94] This model risks creating an enforcement gap where non-compliant ADM continues until challenged, placing the responsibility on data subjects rather than controllers.

Another key consideration is the effect of these interpretations on the right to explanation. If section 71 is a prohibition, then only lawful ADM under section 71(2) would occur, and section 71(3) would ensure that data subjects receive sufficient information to understand the logic behind the decisions affecting them.[95] However, if section 71 is merely a right to object, then ADM could be conducted without meeting section 71(2) requirements until an objection is raised. This loophole could allow non-compliant ADM to escape scrutiny and avoid transparency obligations unless a data subject takes action.[96]

Under the prohibition model, responsible parties would be legally bound to limit ADM to the specified circumstances in section 71(2) before engaging in such processing.[97] This ensures greater protection for individuals, reducing the risk of unlawful or opaque decision-making. By contrast, if section 71 is viewed as a right to object, restrictions on ADM would only apply when

---

[84] Thouvenin, "Article 22 GDPR," 183–190.
[85] Wachter, "Why a Right to Explanation," 94–95.
[86] Wachter, "Why a Right to Explanation," 94–95.
[87] The Article 29 Working Party and the EDPB have expressed the view that Article 22(1) establishes a general prohibition. See Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 19–20.
[88] Wachter, "Why a Right to Explanation," 94–96.
[89] Roos, "Data Protection Principles," 5–7.
[90] POPIA, sec. 71(1).
[91] Article 29 Working Party, *Guidelines on Automated Individual Decision-making*, 21–22.
[92] Wachter, "Why a Right to Explanation," 95.
[93] See POPIA, sec. 71(2)(a)–(b) and (3).
[94] Wachter, "Why a Right to Explanation," 95.
[95] POPIA, sec. 18 imposes notification duties on data controllers to provide data subjects with information when personal data is collected and sec. 23 of POPIA also grants the data subjects a right of access to the same information.
[96] See POPIA, sec. 9. The main purpose of the transparency obligations in POPIA is to ensure fair and transparent processing to allow data subjects to be aware of and verify the lawfulness of processing. See also Roos, "Data Protection Principles," 14–19.
[97] Burns, A Commentary on the POPIA, 21. Burns and Burger-Smidt argue that processing must be done in accordance with the law, which means that the responsible party must comply with the law generally.

a data subject formally challenges a decision.[98] This approach could undermine transparency, as individuals might not be aware of automated processing affecting them and therefore might not exercise their right to object.

Ultimately, interpreting section 71 as a prohibition offers stronger safeguards for data subjects by ensuring that ADM is restricted unless explicitly justified.[99] It requires responsible parties to demonstrate compliance before processing occurs rather than requiring individuals to monitor and challenge decisions. By contrast, interpreting section 71 as a right to object shifts the burden onto data subjects, potentially allowing non-compliant ADM to proceed until it is contested.[100] Given the importance of algorithmic transparency and data protection, the prohibition approach better aligns with the principles of fairness and accountability. It ensures that individuals are protected by default rather than requiring them to take action to safeguard their rights.[101]

2.4 What are the Appropriate Measures that the Data Subject is Entitled to?

ADM under section 71 of POPIA is a critical legal safeguard designed to protect individuals from decisions that are made without human intervention and that result in significant consequences.[102] Section 71(1) states that a data subject has the right not to be subject to a decision that is based solely on automated processing if it results in legal consequences or affects them to a substantial degree. The provision aims to ensure that individuals are not unfairly disadvantaged by algorithmic decision-making processes, particularly when these decisions involve profiling based on attributes such as creditworthiness, employment performance, health, or personal preferences.[103]

Another crucial aspect of section 71 is the requirement for "appropriate measures" to protect the data subject's interests. Section 71(2)(a)(ii) provides expressly that these measures must "(a) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and (b) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations." A restrictive reading of section 71(3)(b) could limit these measures to merely providing information about the logic behind the decision and facilitating representations by the data subject. However, a broader interpretation aligns with other sections of POPIA, such as section 16 on data quality, section 17 on documentation of processing activities, and section 18 on notification requirements. Ensuring that personal data is accurate, maintaining documentation of processing activities, and informing the data subject about data collection are all essential safeguards that contribute to transparency and accountability in ADM.[104]

Judicial interpretations of similar provisions in the GDPR have underscored the necessity for meaningful transparency in ADM. In *Dun & Bradstreet***,** the Austrian Administrative Court ruled that individuals have a right under Article 15(1)(h) GDPR to receive accurate and comprehensible information about how their data is processed in ADM systems.[105] The European Court of Justice emphasised that the mere disclosure of an algorithmic formula or code would not suffice. Instead, the responsible party must explain the actual principles applied in a way that allows the data subject to understand how the decision was made and to contest it if necessary.[106] This decision highlights the importance of algorithmic transparency as a prerequisite for accountability.

In the South African context, compliance with section 71(3)(b) of POPIA requires that data subjects be given clear and comprehensible explanations of automated decisions that affect them. While the provision does not explicitly confer a right to explanation, it imposes an obligation on data controllers to provide sufficient information to enable data subjects to challenge

[98] Wachter, "Why a Right to Explanation," 95.
[99] Wachter, "Why a Right to Explanation," 95.
[100] Wachter, "Why a Right to Explanation," 95.
[101] Information Commissioner's Office, "How Do We Ensure Fairness in AI?" According to the Information Commissioner's Office, data protection by design and default requires that responsible parties consider data protection issues at the design stage of their processing and throughout the AI lifecycle. This is also set out in *General Data Protection Regulation (GDPR)*, art. 25.
[102] Section 71(1) provides that *'a data subject may not be subjected 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 automated processing of personal information intended to provide a profile of such person.'* This provision seeks to ensure that individuals are not unfairly disadvantaged by algorithmic processes, particularly where such decisions concern their *creditworthiness, employment performance, health, or personal preferences*.
[103] Goodman, "European Union Regulations," 53.
[104] See POPIA, secs. 16–18.
[105] See Case C-203/22, *Dun & Bradstreet*. In this case, Dun & Bradstreet was in violation of art. 15(1)(h) GDPR because they didn't disclose the information requested by the data subject and they failed to provide reasons justifying the request rejection.
[106] See Case C-203/22, *Dun & Bradstreet*. In this case, Dun & Bradstreet was in violation of art. 15(1)(h) GDPR because they didn't disclose the information requested by the data subject and they failed to provide reasons justifying the request rejection**.**

decisions. Following the reasoning of the CJEU in *Dun & Bradstreet*, explanations should be aligned with the specific decision taken, ensuring that data subjects are not merely presented with generic information but are given insights that allow them to contest or understand the decision's impact on them.[107]

Ultimately, the right to an explanation serves as a crucial mechanism for ensuring fairness and accountability in ADM.[108] Without clear guidance on the meaning of "affects to a substantial degree" and without robust obligations on responsible parties to provide transparent and meaningful explanations, there is a risk that ADM could result in opaque and potentially discriminatory decision-making processes.[109] Section 71 of POPIA provides an important framework for regulating ADM, but its effectiveness depends on a purposive interpretation that upholds the rights of data subjects and ensures that appropriate measures are implemented to mitigate the risks associated with algorithmic decision-making.

3. Does POPIA Provide the Data Subject the Right to an Explanation?

POPIA does not explicitly grant data subjects a definitive right to an explanation regarding ADM. However, the interpretation of section 71 raises the question of whether such a right can be inferred. Comparisons to the GDPR and the Artificial Intelligence Act provide insights into the types of explanations that may be considered necessary in the context of ADM.[110]

Under the GDPR, the right to an explanation remains a contested issue. While Article 22 provides data subjects with rights in relation to ADM, scholars such as Wachter et al argue that the GDPR does not impose a clear obligation on data controllers to provide meaningful explanations to affected individuals.[111] They contend that while the GDPR includes transparency obligations, these fall short of establishing a true right to explanation.[112]

Furthermore, they argue that Articles 13–15 of the GDPR primarily establish a right to be informed, which requires the data controller to provide information about the logic involved, as well as the significance and envisaged consequences of ADM systems.[113] However, they argue that this obligation focuses on general system functionality and is an *ex-ante* requirement to inform data subjects before or during data collection rather than an *ex-post* right to explanation of a specific decision after it has been made.[114]

Two main criteria can be used to assess explanations: timing and content. Timing distinguishes between *ex-ante* explanations (provided before an automated decision is made) and *ex-post* explanations (offered after the decision has been reached).[115] Content-based explanations can focus on either system functionality (the logic, significance, and consequences of the ADM system) or specific decisions (rationale and factors influencing a particular outcome).[116]

POPIA does not provide explicit guidance on the nature of explanations that data subjects may receive. However, if section 71 is interpreted in alignment with GDPR principles, the following three types of explanations could be relevant:

- *ex-ante* explanation of system functionality (generic explanation before a decision is made);[117]
- *ex-post* explanation of system functionality (generic explanation after a decision is made); and[118]
- *ex-post* explanation of a specific decision (a tailored explanation of the rationale for a particular outcome).[119]

[107] As above. Opinion of Advocate General De la Tour in *Dun & Bradstreet*. Here the AG clarified that the information about the automatic decision-making process disclosed to a data subject needs to be compliant with the transparency requirement, based on such information, a data subject should be able to understand the process leading to the decision made.
[108] As above. The CJEU confirmed that the controller should find simple ways to inform the data subject about the rationale or criteria used in reaching the automated decision so that the data subject can understand how their personal information was used to make the decision.
[109] Zarsky, "The Trouble with Algorithmic Decisions," 124–126.
[110] The *Artificial Intelligence Act*, art. 86 explicitly formulates a right to an explanation for individuals affected by decisions made by specific high-risk AI systems. The right is triggered when the AI system makes a decision that significantly affects a person.
[111] Wachter, "Why a Right to Explanation," 76–80.
[112] Wachter, "Why a Right to Explanation," 76–80.
[113] Wachter, "Why a Right to Explanation," 78.
[114] Wachter, "Why a Right to Explanation," 78.
[115] Burrell, "How the Machine 'Thinks'," 3–4. See also Lu, "Data Privacy," 2098 and Rudin and Radin, "Why Are We Using Black Box Models," 3.
[116] Kim, "Why a Right to an Explanation," 79–83. See also Wachter, "Why a Right to Explanation," 79.
[117] Wachter, "Why a Right to Explanation," 78–80.
[118] Wachter, "Why a Right to Explanation," 79.
[119] Kim, "Why a Right to an Explanation," 79–83.

An *ex-ante* explanation primarily concerns system functionality, covering aspects such as decision trees, predefined models, and classification structures.[120] Since a specific decision has not yet been made, this type of explanation focuses on general operational principles rather than individualised justifications.[121] In contrast, an *ex-post* explanation can provide insights into both system functionality and the specific reasons behind a decision.[122] This latter category includes details on weighting criteria, profiling factors, and the impact of machine-defined rules on the outcome.

The broader purpose of an explanation influences the depth of information provided. Courts have, in *Schufa* and *Dun & Bradstreet*, required data controllers to furnish individuals with enough information to contest an ADM decision effectively.[123] This interpretation aligns with the right to contest and the right to be heard, as outlined in Article 22(3) and Recital 71 of the GDPR. Some legal scholars, such as Sarra, argue that the right to contest should be viewed as the highest safeguard within the framework of ADM regulation.[124] If this perspective is adopted, data controllers would be compelled to provide detailed explanations to meet a higher legal threshold for transparency and accountability. However, the transferability of the EU's approach to South Africa must be understood within the distinct constitutional and cultural context of each jurisdiction.

Additionally, the right to an explanation can be linked to fundamental legal principles, such as the right to an effective remedy under Article 47 of the *Charter of Fundamental Rights of the European Union*.[125] A parallel can be drawn with Article 9 of the *African Charter on Human and Peoples' Rights*, which provides that 'every individual shall have the right to receive information.' This perspective suggests that explanations should not merely be procedural formalities but should provide substantive insights that empower individuals to challenge and rectify unfair or biased decisions.[126]

In the context of POPIA, the argument for an implied right to explanation can draw upon these interpretations of GDPR provisions. While POPIA does not explicitly mandate a right to an explanation, responsible parties may be expected to offer one if the data subject wishes to contest an ADM decision.[127] If section 71 is interpreted as a prohibition on ADM unless specific conditions are met, responsible parties would need to ensure transparency by providing explanations in compliance with legal requirements.[128] However, if section 71 is viewed merely as a right to object, the obligation to explain decisions may only arise if a data subject actively challenges the outcome.[129]

In conclusion, while POPIA does not explicitly guarantee a right to an explanation, similar principles from the GDPR can be applied to argue that explanations should be provided, particularly when individuals contest automated decisions. The distinction between system functionality explanations and specific decision explanations remains critical, with *ex-ante* and *ex-post* frameworks shaping the depth of transparency required. Given the increasing use of ADM in various sectors, the legal interpretation of section 71 should ideally align with fairness and accountability principles, ensuring that data subjects receive meaningful information about decisions that significantly affect them.

[120] Kim, "Why a Right to an Explanation," 79–83.
[121] Kim, "Why a Right to an Explanation," 79–83.
[122] Kim, "Why a Right to an Explanation," 79–83.
[123] See Case C-634/21, *SCHUFA Holding* and Case C-203/22, *Dun & Bradstreet.* See also Silveira, "Automated Individual Decision-Making," 75.
[124] Sarra, "Artificial Intelligence in Decision-making," 45–62.
[125] Article 47 of the Charter guarantees the right to an effective remedy and a fair trial for individuals whose rights under Union law have been violated. It ensures access to an independent and impartial tribunal for a fair and public hearing within a reasonable timeframe. In addition, it grants the right to legal representation and assistance. For those without sufficient financial means, legal aid must be provided to ensure equal access to justice.
[126] Malgieri, "Why a Right to Legibility," 247.
[127] Brand, "Responsible Artificial Intelligence," 142–145.
[128] Wachter, "Why a Right to Explanation," 78.
[129] Wachter, "Why a Right to Explanation," 78.

4. Recommendations for Strengthening POPIA's Protections

To enhance the effectiveness of section 71 and prevent circumvention through superficial human intervention, the following recommendations should be considered:

4.1 Clarification of 'Solely Automated' Decisions

Section 71 should be amended to define what constitutes meaningful human oversight. Without clear criteria, tokenistic human involvement may be used to bypass the restrictions on ADM.[130] A substantive human review should include independent reasoning, the ability to override automated outcomes, and accountability mechanisms.[131]

4.2 Introduction of a Right to Explanation

Responsible parties should be required to provide clear, accessible explanations of how algorithmically-generated decisions are reached.[132] This includes disclosure of key factors influencing the decision and a distinction between generic system functionality explanations and case-specific rationales.[133] Establishing an explicit right to explanation in POPIA would align it with global best practices and improve transparency for data subjects.

4.3 Enhanced Oversight Mechanisms

Section 107 of POPIA prescribes fines of up to R10 million or imprisonment of up to ten years for serious offences, reflecting the legislature's intent to promote compliance through deterrence. However, these provisions remain reactive, focusing on punishment after non-compliance rather than ensuring proactive accountability. To strengthen accountability, POPIA should incorporate stronger auditing and accountability measures to assess whether human involvement in decision-making is substantive.[134] This could include periodic evaluations of ADM systems, regulatory reporting obligations, and requiring organisations to demonstrate that human oversight is meaningful rather than a procedural formality.[135]

4.4 Alignment with International Best Practices

POPIA's protections should be aligned with evolving interpretations of ADM under the GDPR and other international frameworks.[136] Comparative analysis with the European approach can inform improvements, particularly regarding the right to contest automated decisions and the role of fundamental rights in determining the adequacy of explanations provided to data subjects.[137]

5. Conclusion

The interpretation of section 71 of POPIA has significant implications for the rights of data subjects and the accountability of responsible parties involved in ADM. If viewed as a right to object, it places the burden on individuals to be aware of and challenge automated decisions that may impact them. Conversely, a prohibition-based approach would provide stronger safeguards by ensuring that ADM is restricted unless explicitly justified under section 71(2). A blended approach, which recognises both the prohibitive and participatory dimensions of section 71, could offer a more balanced framework. This could ensure that ADM is permitted only under defined circumstances while still empowering data subjects to contest or seek explanations for such decisions. Adopting a dual model would promote both regulatory oversight and individual agency, enhancing fairness and accountability in ADM.

A key consideration in this debate is the right to an explanation. While POPIA does not currently provide explicit guidance on the type of explanation data subjects are entitled to, international scholarship and interpretations of GDPR suggest that meaningful explanations can be categorised based on timing (*ex-ante* or *ex-post*) and content (generic system functionality or specific decision rationale). Strengthening POPIA to require such explanations would enhance transparency and empower data subjects to contest unfair or opaque decisions.

---

[130] Mendoza, "The Right Not to Be Subject," 87.
[131] Wagner, "Liable, but Not in Control?," 118.
[132] Casey, "Rethinking Explainable Machines," 146.
[133] Casey, "Rethinking Explainable Machines," 146.
[134] Casey, "Rethinking Explainable Machines," 146.
[135] Casey, "Rethinking Explainable Machines," 146.
[136] A broad interpretation should be given to *General Data Protection Regulation (GDPR)*, arts. 15 and 22 and POPIA, sec. 71(3).
[137] Wagner, "Liable, but Not in Control?," 118.

The prohibition model offers greater protections by requiring responsible parties to justify ADM before processing occurs, reducing the risk of non-compliant or unaccountable decision-making. Strengthening section 71 through clearer definitions, a right to explanation, enhanced oversight mechanisms, and alignment with international best practices would ensure that South Africa's data protection framework remains robust and adaptive in an era of increasing reliance on ADM.

Bibliography

Legal Materials

Article 29 Data Protection Working Party. *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*. WP 251 rev.01. 2018.

Charter of Fundamental Rights of the European Union. 2012 O.J. (C 326) 391.

Court of Justice of the European Union. *Dun & Bradstreet Austria GmbH v Kriminálny úrad finančnej správy*. ECLI:EU:C:2024:218. March 7, 2024.

Court of Justice of the European Union. *SCHUFA Holding AG v. C-634/21*. ECLI:EU:C:2023:957. December 7, 2023.

Court of Justice of the European Union. Opinion of Advocate General Pikamäe in *SCHUFA Holding*. ECLI:EU:C:2023:220. March 16, 2023.

European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016 O.J. (L 119) 1.

European Parliament and Council of the European Union. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Laying Down Harmonised Rules on Artificial Intelligence and Amending certain Union Legislative Acts (Artificial Intelligence Act)*. 2024 O.J. L, 2024/1689.

South Africa. Constitutional Court. *Brümmer v Minister for Social Development*. 2009 (6) SA 323 (CC).

South Africa. Constitutional Court. *Investigating Directorate v Hyundai Motor Distributors; In re: Hyundai Motor Distributors v Smit NO*. 2001 (1) SA 545 (CC).

South Africa. Constitutional Court. *S v Makwanyane*. 1995 (3) SA 391 (CC).

South Africa. Gauteng Division of the High Court. *Arena Holdings (Pty) Ltd t/a Financial Mail v South African Revenue Services*. 2022 (2) SA 485 (GP).

South Africa. Western Cape Division of the High Court. *Tiso Blackstar Group (Pty) Ltd v Steinhoff International Holdings N.V.* 2023 (1) SA 283 (WCC)

South Africa. *Protection of Personal Information Act 4 of 2013 (POPIA)*. Statutes of the Republic of South Africa.

Secondary Materials

Adewoyin, Musa Adekunle, Olugbenga Adediwin and Audu Joseph Audu. "Artificial Intelligence and Sustainable Energy Development: A Review of Applications, Challenges, and Future Directions." *International Journal of Multidisciplinary Research and Growth Evaluation* 6, no 2 (2025): 196–203. https://doi.org/10.54660/.IJMRGE.2025.6.2.196-203.

Allen, Robin and Dee Masters. "Artificial Intelligence: The Right to Protection from Discrimination Caused by Algorithms, Machine Learning and Automated Decision-Making." *ERA Forum* 20, no 4 (2020): 585–598. https://doi.org/10.1007/s12027-019-00582-w.

Brand, Donrich. "Responsible Artificial Intelligence in Government: Development of a Legal Framework for South Africa." *JeDEM-journal of eDemocracy and Open Government* 14, no 1 (2022): 139–159. https://doi.org/10.29379/jedem.v14i1.678.

Burns, Yvonne and Alida Burger-Smidt. *A Commentary on the Protection of Personal Information Act*. Durban: LexisNexis, 2018.

Burrell, Jenna. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." *Big Data and Society* 3, no 1 (2016): 1–12. https://doi.org/10.1177/2053951715622512.

Casey, Bryan, Ashkon Farhangi and Roland Vogl. "Rethinking Explainable Machines." *Berkeley Technology Law Journal* 34, no 1 (2019): 1–68. https://doi.org/10.15779/Z38B56D64T.

Dimitrova, Diana. "The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and beyond the GDPR." *European Data Protection Law Review* 6, no 2 (2020): 211–230. https://doi.org/10.21552/edpl/2020/2/8.

Edwards, Lilian, and Michael Veale. "Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions?'" *IEEE Security and Privacy* 16, no 3 (2018): 48–57. https://doi.org/10.1109/MSP.2018.2701152.

Francis, David and Edward Webster. "Poverty and Inequality in South Africa: Critical Reflections." *Development Southern Africa* 36, no 6 (2019): 788–789. https://doi.org/10.1080/0376835X.2019.1666703.

Goodman, Bryce, and Seth Flaxman. "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation.'" *arXiv* preprint, June 2016. http://arxiv.org/abs/1606.08813.

Green, Ben. "The Flaws of Policies Requiring Human Oversight of Government Algorithms." *Computer Law and Security Review* 45 (2022): 102326. https://doi.org/10.1016/j.clsr.2022.105681.

Information Commissioner's Office. "Guidance on AI and Data Protection." Accessed June 26, 2025. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

Information Commissioner's Office. "Rights Related to Automated Decision Making and Profiling." Accessed June 26, 2025. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/rights-related-to-automated-decision-making-and-profiling/.

Johnson, Kristin, Frank Pasquale and Jennifer Chapman. "Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation." *Fordham Law Review* 88 (2019): 499–517. https://ir.lawnet.fordham.edu/flr/vol88/iss2/5/.

Kim, Tae Wan and Bryan R. Routledge. "Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach." *Business Ethics Quarterly* 32, no 1 (2022): 73–105. https://doi.org/10.1017/beq.2021.3.

Kleinberg, Jon, Jens Ludwig, Sendhil Mullainathan and Cass R. Sunstein. "Discrimination in the Age of Algorithms." *Journal of Legal Analysis* 10 (2018): 124–144. https://doi.org/10.1093/jla/laz001.

Lu, Shirley. "Data Privacy, Human Rights, and Algorithmic Opacity." *California Law Review* 110 (2022): 2079–2106.

Malgieri, Gianclaudio and Giovanni Comandé. "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation." *International Data Privacy Law* 7, no 4 (2017): 243–269. https://doi.org/10.1093/idpl/ipx019.

Mendoza, Isak and Lee A. Bygrave. "The Right Not to Be Subject to Automated Decisions Based on Profiling." In *European Union Internet Law: Regulation and Enforcement*, edited by Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou, and Thalia Prastitou, 81–98. Cham: Springer, 2017.

Metikoš, Ljubiša and Jef Ausloos. "The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act." *Law, Innovation and Technology* (forthcoming 2025). https://doi.org/10.1080/17579961.2025.2469349.

Miao, Michelle. "Debating the Right to Explanation: An Autonomy-Based Analytical Framework." *South African Journal of Criminal Justice* 34 (2022): 876–877.

Naudts, Lauren, Pierre Dewitte and Jef Ausloos. "Meaningful Transparency through Data Rights: A Multidimensional Analysis." In *Research Handbook on EU Data Protection Law*, edited by Eleni Kosta and Franziska Boehm, 530–571. Cheltenham, UK: Edward Elgar Publishing, 2022.

Orthofer, Anna. "Wealth Inequality in South Africa: Evidence from Survey and Tax Data." *Research Project on Employment, Income Distribution & Inclusive Growth*, no 15 (2016): 1–5.

Remolina, Nydia. "The Role of Financial Regulators in the Governance of Algorithmic Credit Scoring." Working Paper, Social Science Research Network, 2022.

Roos, Anneliese. "Data Protection Principles under the GDPR and the POPI Act: A Comparison." *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 86 (2023): 5–7.

Rudin, Cynthia, and Joanna Radin. "Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson from an Explainable AI Competition." *Harvard Data Science Review* 1, no 2 (2019). https://doi.org/10.1162/99608f92.5a8a3a3d.

Rudin, Cynthia. "Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead." *Nature Machine Intelligence* 1, no 5 (2019): 206–215. https://doi.org/10.1038/s42256-019-0048-x.

Sampene, Agyemang K., Fredrick Oteng Agyeman, Robert Brenya and John Wiredu. "Artificial Intelligence as a Pathway to Africa's Transformations." *Artificial Intelligence* 9, no 1 (2022): 14939–14951.

Sarra, Christos. "Artificial Intelligence in Decision-making: A Test of Consistency between the 'EU AI Act' and the 'General Data Protection Regulation'" *Athens Journal of Law* 11, no 1 (2025): 45–62. https://doi.org/10.30958/ajl.11-1-3.

Selbst, Andrew D. and Solon Barocas. "The Intuitive Appeal of Explainable Machines." *Fordham Law Review* 87 (2018): 1085–1139.

Silveira, Alessandra. "Automated Individual Decision-Making and Profiling [on Case C-634/21-SCHUFA (Scoring)]." *UNIO–EU Law Journal* 8, no 2 (2023): 71–79. https://doi.org/10.21814/unio.8.2.534.

Singh, Sachil F. "Social Sorting as 'Social Transformation:' Credit Scoring and the Reproduction of Populations as Risks in South Africa." *Security Dialogue* 46, no 4 (2015): 365–383. https://doi.org/10.1177/0967010615583034.

Temme, Merle. "Algorithms and Transparency in View of the New General Data Protection Regulation." *European Data Protection Law Review* 3 (2017): 475–477. https://doi.org/10.21552/edpl/2017/4/13.

Thouvenin, Florent, Alfred Fruh, and Stefan Henseler. "Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?" *European Data Protection Law Review* 8 (2022): 183–190. https://doi.org/10.21552/edpl/2022/2/10.

Townsend, Beverley A., and Donrich W. Thaldar. "Navigating Uncharted Waters: Biobanks and Informational Privacy in South Africa." *South African Journal on Human Rights* 35, no 4 (2019): 342–360.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7, no 2 (2017): 76–99. https://doi.org/10.1093/idpl/ipx005.

Wagner, Ben. "Efficiency vs. Accountability? Algorithms, Big Data and Public Administration." In *Building Blocks for a Digital Future*, 12–18. Amsterdam: Bureau de Helling, 2016.

Wagner, Ben. "Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems." *Policy and Internet* 11, no 1 (2019): 105–122. https://doi.org/10.1002/poi3.198.

Wiedemann, Kai. "Profiling and (Automated) Decision-Making under the GDPR: A Two-Step Approach." *Computer Law and Security Review* 45 (2022): 102360. https://doi.org/10.1016/j.clsr.2022.102360.

Zarsky, Tal. "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making." *Science, Technology and Human Values* 41, no 1 (2016): 118–132. https://doi.org/10.1177/0162243915605575.