11 The regulation of automated decision making and profiling in an era of big data and ambient intelligence: A European and South African perspective

Alon Lev Alkalay

Abstract

The twenty-first century presents a challenge to human liberties as automated decision-making (ADM) and profiling technologies advance. Enabled by big data (BD) and machine learning (ML), these technologies delve into 'invisible knowledge,' with the capability to manipulate human emotions and behaviours. The looming era of ambient intelligence (AmI) amplifies these concerns by seamlessly integrating computing and biometric technologies into environments. Regulatory efforts such as the GDPR and POPIA signal recognition of these challenges but fall short in addressing evolving technological landscapes. This chapter scrutinises EU and South African data protection laws, assessing their adequacy in the face of ADM and profiling in BD and AmI contexts. Through conceptual analysis and comparison, it aims to illuminate regulatory shortcomings and propose pathways for governance in an era defined by algorithmic influence.

1 Introduction

Whether or not we are conscious of (or care to acknowledge) it, humans are organisms, 'organisms are algorithms'[1], and algorithms can be 'hacked'.[2] On this note, two pervasive technological developments – and the technical processes of automated decision making (ADM) and profiling that they facilitate – will pose a challenge to the assurance of human liberties in the twenty-first century. Today, the confluence of a data-driven information society; exponentially increasing levels of processing power; limitless cloud storage and ML algorithms have resulted in an era of big data (BD).[3]

1 See YN Harari *Homo Deus: A brief history of tomorrow* (2016) 383. See also YN Harari *21 Lessons for the 21st Century* (2018) 47.

2 'Hacked' in this instance refers to unauthorised access to the inner workings of the human mind and body.

3 'Big data' may be understood as 'novel ways in which organi[s]ations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations'. See IS Rubenstein 'Big data: The end of privacy or a new beginning?' (2013) 3 *International Data Privacy Law* 74.

Thereunder, the abilities to (i) make automated decisions concerning humans; and (ii) manipulate human emotions, perceptions, behaviours, preferences and habits, are being fostered by entities that are learning to know us better than we understand ourselves as a result of the extraction and utilisation of 'invisible knowledge'[4] hidden within large sets of data. We are, after all, algorithms at our core.

Tomorrow, an era of ambient intelligence (AmI)[5] has been envisioned[6] that will build upon BD processing by injecting a combination of autonomic, omnipresent computing[7] and 'second generation'[8] biometric technologies into smart, sensor-rich environments that are 'capable of recognising and responding to individuals in a seamless, unobtrusive and invisible way'[9] by preemptively adapting to human preferences.[10] Hildebrandt and Koops describe these intelligent environments as being akin to 'digital butler[s]'.[11]

Whereas BD has already facilitated automated decision making (ADM) capabilities and profiling practices, an era of AmI – despite having the potential to positively impact many aspects of life – will elevate and proliferate these processes and broaden their potential impact on fundamental human liberties as a result of unseeable 'prejudicial computations'.[12] Consequentially, the regulation of automated processes – which has already begun in the European Union (EU) under its General

4 See M Hildebrandt 'Who is profiling who? Invisible invisibility' in S Gutwirth and others (eds) *Reinventing data protection?* (2009) 239.

5 M Hildebrandt 'Profiling and AmI' in K Rannenberg, D Royer & A Deuker (eds) *The future of identity in the information society: Challenges and opportunities* (2009) 286.

6 AmI is a European conceptualisation by the European Information Society Technologies Advisory Group (ISTAG). In other parts of the world, similar conceptualisations take the form of 'ubiquitous computing' (United States of America) and 'ubiquitous networking' (Japan), for example. See SE Bibri *The shaping of ambient intelligence and the internet of things* (2015) 89.

7 Hildebrandt (n 5) 288.

8 Instead of identifying 'who you are', second generation biometrics focus on determining 'how you are' in relation to your environment. For a detailed investigation into second generation biometrics, see E Mordini & D Tzovaras (eds) *Second generation biometrics: The ethical, legal and social context* (2012) 11.

9 D Wright, S Gutwirth & M Friedewald (eds) *Safeguards in a world of ambient intelligence* (2008) 1.

10 M Hildebrandt & B-J Koops 'The challenges of ambient law and legal protection in the profiling era' (2010) 73 *Modern Law Review* 431.

11 As above.

12 The phrase 'prejudicial computations' is used here to refer to mathematical and statistical outcomes, inferences or decisions that are either used to create/apply a profile, or make an automated decision in regard to a data subject.

Data Protection Regulations 2016/679 (GDPR)[13] and in South Africa under its Protection of Personal Information Act 4 of 2013 (POPIA)[14] – has become a topic of increasing discussion among academia and policy makers abroad, signifying the relevance of contributing to, and continuing this discussion within a South African context.

Considering the foregoing, in this chapter[15] I will seek to explore the extent of EU and South African data protection laws and their adequacy in light of the ethical and legal issues that may arise from ADM and profiling practices in an era of BD and AmI. Ultimately, I will aim to highlight that despite recent overhauls, the current state of data-protection law – utilising the EU and South Africa as jurisdictional yardsticks – contains fundamental flaws that significantly impact on its adequacy in an era of BD and AmI.

This chapter is divided in five parts. I begin the exploration in part 2 by conceptualising and differentiating ADM and profiling to enable a proper analysis of the laws under consideration. Thereafter, in part 3 I unpack and compare the definitions, semantics, and provisions of GDPR and POPIA in order to assess the extent of their regulative postures towards ADM and profiling. In part 4 I consider the adequacy of these laws today (in the context of BD), and tomorrow (in the context of AmI) and thereafter collate and build upon recommendations that have been posited for the future regulation of ADM and profiling. Finally, in part 5 I provide concluding remarks as to the findings of the exploration undertaken through this chapter.

13 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.

14 Protection of Personal Information Act 4 of 2013 (POPIA).

15 I note two limitations to the scope of this chapter. First, the chapter will exclusively concern itself with solely automated ADM and profiling practices, conducted by non-state entities (with an emphasis on corporations). Second, while it is acknowledged that ADM and profiling technologies may be subject to constitutional scrutiny, the chapter primarily focuses on the extent and adequacy of laws provided at a statutory level – specifically in regard to GDPR and POPIA. Accordingly, the manner in which consumer protection, anti-discrimination and equality, and artificial intelligence laws eg, may impact ADM and profiling practices, will not be considered herein. Finally, I acknowledge that specific terminological differences exist between GDPR and POPIA. Having said that, throughout this chapter I shall primarily make use of terminology contained in POPIA, except where I am specifically discussing GDPR.

2 Conceptualising and differentiating automated decision making from profiling

In order to properly explore the extent and adequacy of the current regulation of ADM and profiling, one must understand the manner in which these technological processes function and relate with one another. Accordingly, before conceptualising ADM and profiling in their own right, I wish to note three over-arching dynamics that bear an impact on the regulation of these processes – all of which will be canvassed more fully across parts 3 and 4.

First, despite being distinct processes that may take place independently, ADM and profiling are often interrelated. In many instances, decisions are reached by applying profiles, while profiles may also be constructed by considering a set of automated decisions – they may, therefore, feed into one another.

Second, both ADM and profiling may, or may not (where human control is involved) be solely automated – resultantly, EU and South African legislators have adopted what I regard as a 'two-prong approach' to these processes, so as to regulate solely automated instances and those including human involvement, separately.

Third, both ADM and profiling may, or may not, involve the processing of 'personal information'. Where 'group profiles' or 'de-identified' personal information are involved, a significant lacuna arises in the laws under consideration.[16]

2.1 Automated decision making

In its simplest form, ADM may be regarded as the arrival at a decision by a computer system, made autonomously, without human involvement.[17] Logically, for a decision to be made autonomously, it must be based upon data, which may be either (i) collected; (ii) observed; or (iii) inferred.[18] The

16 S Gutwirth & P de Hert 'Regulating profiling in a democratic constitutional state' in M Hildebrandt & S Gutwirth *Profiling the European citizen: Cross-disciplinary perspectives* (2008) 288.

17 Art 29 Data Protection Working Party (251rev.01) *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (2017) 8.

18 As above.

various sources of data that ADM can be based upon the application of profiles but need not necessarily be.[19]

2.2 Profiling

'Profiling' is not a concept isolated to the realms of information technology. In fact, humans and animals profile the world every day.[20] However, insofar as this chapter is concerned – and the laws that I seek to explore – I posit a working definition of 'profiling' as 'the process of using algorithms to *construct* "probabilistic knowledge" (inferences/predictions) through the discovery of correlations in large datasets, which knowledge may be *applied* by identifying, representing or making decisions about, an individual or group of data subjects'.[21]

For the sake of clarity, I will extrapolate two core elements from the above working definition. First, profiles can be both 'constructed' (inferred from data) and 'applied' (through identification, representation or in the course of decision making).[22] Second, any construction or application of a profile can be carried out both 'individually' (upon specific data subjects) as well as 'collectively' (upon groups of anonymous data subjects – 'group data')[23]. Further, their application can be direct (upon the same data subject to whom the profile relates) or indirect (where a profile from another person or group is applied to the data subject).[24] Importantly, when profiles are applied, new profiles may be created that may then enter a feedback loop of profile application and profile creation to 'mine' further 'knowledge'. The legal issues relating to indirect 'group profiling' will be clarified in part 4.

19 Example: A driver receives a traffic fine for speeding measured by an average-speed-over-distance camera. In this instance, the mere evidence that the driver sped resulted in an automated decision about the driver's road conduct. No profile was applied when reaching the automated decision. Yet, it is plausible that a system may assess a driver's conduct over time (creation of a profile), which profile may then be applied (either manually or autonomously) when determining the quantum of the driver's fine.

20 M Hildebrandt 'Defining profiling: A new type of knowledge' in M Hildebrandt & S Gutwirth *Profiling the European citizen: Cross-disciplinary perspectives* (2008) 25-27.

21 Hildebrandt (n 21) 19 (my emphasis).

22 Hildebrandt (n 21) 18.

23 Hildebrandt (n 21) 20-21.

24 Hildebrandt (n 21) 34-35.

As eluded to above, in practice the lines between decision making and profiling can blur, which has led some legal scholars to perceive the profiling process more broadly as including the making of decisions.[25] While profiles may be applied during decision making, this is not their only function – for example, profiles may be created and applied to other profiles when identifying or representing data subjects or a group. Accordingly, the making of a decision based on a profile is a separate activity that falls within the domain of decision making or ADM. In the former case, profiling is an algorithmic process to find new 'knowledge' and uncover 'patterns' or 'correlations', whereas in the latter case, the application of a profile for decision making is not.

3 Exploring the extent of regulation under GDPR and POPIA

3.1 Primary legal instruments

3.1.1 European Union

Statutory protection against the unlawful processing of personal data – which implicitly includes unlawful ADM and profiling practices – is principally rooted in article 8 of the Charter of Fundamental Human Rights of the European Union 2009,[26] titled 'protection of personal data'. Interestingly, the regulation of ADM had been considered by EU legislators 14 years prior under article 15 of the Data Protection Directive (DPD).[27] However, as Savin puts it, the provisions contained in the DPD, 'although introduced in a technically neutral manner, [were] in need of modernisation'.[28]

In response, a set of Regulations were enacted in the form of GDPR. Having been in force since 25 May 2018, GDPR repealed the DPD and standardised data-protection laws across EU member states. Accordingly, GDPR is now the sole regulatory instrument in the EU overseeing ADM and profiling practices. Where controllers engage in unlawful ADM or profiling practices, they may be fined up to 4 per cent of their worldwide

25 See, eg, D Kamarinou, C Millard & J Singh 'Machine learning with personal data' in R Leenes, R van Brakel & S Gutwirth (eds) *Data protection and privacy: The age of intelligence machines* (2017) 97.

26 Charter of Fundamental Human Rights of the European Union 2012/C 326/02.

27 Directive 95/46/EC of the European Parliament of 24 October 1995.

28 A Savin 'Profiling in the present and new EU data protection frameworks' in PA Nielsen, PK Schmidt & K Dyppel Weber (eds) *Erhvervsretlige emne* (2015) 253.

annual turnover or may be liable for civil damages.[29] In terms of article 3, GDPR also has a notoriously vast territorial application – thus in certain instances providing data subjects within the EU with protection against unlawful ADM and profiling practices by foreign controllers.

Before moving on, I wish to stress that while GDPR is a regulation (and therefore binding), the contents of its Recitals are not legally binding and 'do not have any autonomous legal effect'[30] – unlike the operative provisions of its articles. Jurisprudence before the European Court of Justice (ECJ) has confirmed that Recitals do not confer a right,[31] nor do they restrict a right.[32] Saying that, and without deviating into the academic discourse on the purpose of Recitals in EU law,[33] I will, for the analysis that follows below, note two points. First, an EU court will only consider Recitals to 'dissolve ambiguity'[34] – they, therefore, serve a resolutive function and can indirectly shape future law through judicial interpretation. In this regard, until GDPR's provisions on ADM and profiling come before a European court for interpretation, the operative provisions of GDPR are the primary indicators of the nature and extent of EU regulation. Second, in the context of GDPR (which, as already indicated, is the baseline data protection law for all EU member states), Recitals will serve an important 'role in transposition'[35] when, or if, EU member states codify GDPR's operative provisions into their respective national laws. Accordingly, in what follows below, I will only refer to relevant Recitals to indicate possible interpretive outcomes that may arise in future case law on the provisions under exploration.

3.1.2 Republic of South Africa

In South Africa, the unjustified collection of personal information about an individual is regarded by its common law as a breach of individual

29 GDPR arts 82 and 83(5), respectively.

30 R Baratta 'Complexity of EU law in the domestic implementing process' (2014) 2 *TTPL* 293.

31 *Criminal Proceedings against Nilsson, Hagelgren & Arrborn* (Case C-162/97) 1998 ECR I-07477.

32 *Giuseppe Manfredi v Regione Puglia* (Case C-308/97) 1998 ECR I-7685.

33 An in-depth exploration of the role of recitals in EU law may be found in T Klimas & J Vaiciukaite 'The law of recitals in European community legislation' (2008) 15 *ILSA Journal of International & Comparative Law* 61.

34 S Wachter, B Mittelstadt & L Floridi 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2017) *International Data Privacy Law* 20.

35 *Giuseppe Manfredi* (n 33) 31.

privacy[36] – which is broadly protected in section 14 of the Constitution of the Republic of South Africa, 1996. Unlike the EU, the comprehensive protection of personal information under data protection law had only recently been introduced in the form of POPIA, which to a significant extent is predicated on the DPD.[37] Under the POPIA, responsible parties may be sanctioned with fines of up to ten million rand for failing to comply with an enforcement notice,[38] or civil damages. Notably, POPIA only applies to processing that takes place within the borders of South Africa.[39]

3.2 What is regulated? Statutory definitions and semantics

3.2.1 GDPR

GDPR governs the processing[40] and movement of 'personal data' by 'data controllers'[41] which it defines as constituting '*any* information relating to an *identified* or *identifiable* natural person'.[42] The scope of personal data has not evolved since the DPD,[43] and while it may remain broad enough to include 'any' information, such information is limited to 'identifiable', 'living',[44] 'natural persons'. Under the same definition, a data subject will be 'identifiable' if that data subject can be identified (either directly or indirectly) through an identifier, or by means of 'factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[45] The definition indirectly provides that de-identified personal data, or data relating to a data subject in group data, may be considered 'personal data' if it can be re-identified usually through a process of reverse engineering where a data subject can be indirectly identified by combining attributes that may appear to be harmless in

36 See *S v Bailey* 1981 (4) SA 187 W; *O'Keeffe v Argus Printing and Publishing Co Ltd & Another* 1945 (3) SA 244 (C).

37 Y Burns & A Burger-Smidt *A commentary on the Protection of Personal Information Act* (2018) 5-6.

38 POPIA secs 103 and 99, respectively.

39 POPIA sec 3(b).

40 Art 4(2) of GDPR defines 'processing' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means'.

41 GDPR art 4(7).

42 GDPR art 4(1) (my emphasis).

43 DPD art 2(a).

44 The definition in art 4(1) does not require that a natural person be 'living'. However, Recital 27 suggests that the scope of GDPR does not extend to deceased persons.

45 GDPR art 4(1).

isolation.[46] While in practice the ability of a controller to re-identify would be up to a data subject to prove, I nonetheless view the meaning conveyed in the definition (as it stands) as having potential to safeguard data subject rights in the face of proliferated de-identification practices (more on this in part 4). However, if a dispute were to arise as to the conflict in the definition, a court would seek to clarify the definition in line with the definition's corresponding Recital. On this note, Recital 26 suggests that for a data subject to be identifiable, the process of re-identification must be 'reasonably likely' to be used. If this suggestion were adopted by a court, it would place a further onus on data subjects to prove, objectively, that a controller was likely to re-identify de-identified personal data or group data. In such a case, data subject rights may be inhibited as a result of a heavy evidentiary burden, and it is on this basis that I view the enforceability of the GDPR definition on 'personal data' as potentially being limited in cases of unfair profiling practices.

In respect of ADM and profiling, both processes are recognised as being distinct under GDPR. ADM may be said to be considered implicitly under the definition of 'processing', which relates to 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means'.[47] Conversely, 'profiling' is explicitly defined as 'any form of automated processing of personal data consisting of the use of personal data to *evaluate* certain personal aspects relating to a natural person, in particular to *analyse* or *predict* aspects concerning that natural [person]'.[48] (emphasis added).

3.2.2 POPIA

The POPIA adopts a slightly nuanced approach to that of the GDPR regarding its semantics. The POPIA applies to all 'processing'[49] of personal information which it defines as 'information relating to an *identi□able*, *living*, *natural* person, and where it is applicable, an *identi□able*, *existing juristic* person'.[50] The definition also includes a widening mechanism under which a non-exhaustive range of personal information may be protected. Unlike GDPR, POPIA does not go on to define what 'identifiable' means in the context of its definition of personal information, or whether the term

46 Contrary to popular belief, re-identification of de-identified data is possible, especially when machine learning algorithms are involved. See Hildebrandt (n 5) 365.

47 GDPR art 4(2).

48 GDPR art 4(4) (my emphasis).

49 Sec 1 of POPIA defines 'processing' as 'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information'.

50 POPIA sec 1.

may be understood to include 'indirect identification' through a reverse engineering process. Accordingly, until a judicial interpretation takes place, the foregoing indicates that de-identified personal information, or the identity of a data subject in group data, that has been, or is capable of being re-identified, is not protected.

Another notable difference in POPIA's approach to personal information is that it extends to 'existing' juristic persons. This extension of protection is a by-product of South African constitutional and common law that extends the right to privacy to juristic persons.[51] In consequence, under POPIA any rights relating to ADM and profiling apply to juristic persons, which is a welcoming development.

Concerning ADM and profiling, POPIA lacks differentiation of the two processes – an oversight that I will show has caused misinterpretations as to POPIA's actual regulatory reach. While neither ADM nor profiling is defined, they both fall under the definition of 'processing' as 'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information'.[52] In fact, the term 'profiling' only appears on two occasions throughout the entire Act – both of which merely relate to POPIA's provisions on ADM.[53] Whether or not POPIA regulates profiling will be considered in parts 3.3.2 and 3.3.4 below.

3.3 How is ADM and profiling regulated? The two-prong approach

Native to the architecture of both GDPR and POPIA is a two-prong approach whereby data subjects are afforded varying rights depending on the circumstances surrounding the processing of their personal information. Fundamentally, both laws broadly regulate all forms of processing, on the one hand (prong one), whilst providing specific regulation for instances that are solely automated (no human involvement – prong two), on the other hand – albeit with their own subtleties and nuances. For explanatory purposes, I will categorise the first prong as providing 'prong one rights' with the second prong providing 'prong two rights'. The first prong broadly relates to all forms of processing of personal information – including ADM and profiling – and is best understood as a 'transparency tool', which Gutwirth describes as not being prohibitive

51 See *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) and *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A), as read with sec 8(4) of the Constitution of the Republic of South Africa, 1996.

52 POPIA sec 1.

53 POPIA sec 5(g) as read with sec 71(1).

but '[aimed] at channelling, regulating and controlling'[54] the processing of personal data in an acceptable, fair manner. Structurally, I view and will address this prong as comprising three elements that seek to instil accountability[55] in responsible parties. These elements are (i) processing principles/conditions;[56] (ii) grounds for lawful processing;[57] and (iii) obligations towards data subjects in respect of any prong one rights they may hold. The second prong exclusively relates to ADM or profiling that is solely automated. Thereunder, over and above 'prong one' rights, data subjects are provided additional 'prong two' rights. Limitations on these prong two rights are also listed, in which case certain 'measures' are required to be put in place by responsible parties to safeguard data subject rights. The second prong is of utmost significance in the context of BD and AmI (more on this in part 4).

Saying that, and before exploring the contents of each prong, I note that a comprehensive discussion of the first prong (which includes the majority of the provisions in GDPR and POPIA) is not possible due to space limitations. While I will provide a complete overview of prong one, I will limit my discussion to the essential aspects therein as they may relate to solely automated ADM and profiling.

3.3.1 GDPR prong one

GDPR's first prong provides for processing principles in article 5, lawful grounds for processing in article 6 and data subject rights in articles 12 to 21. The first prong's processing principles require 'accountability'[58] from controllers who must be able to demonstrate that all processing is (i) lawful, fair and transparent;[59] (ii) undertaken within the bounds of the original specified, explicit and legitimate purpose for which the data was collected;[60] and (iii) accurate.[61] In addition, controllers must comply with

54 Gutwirth & De Hert (n 17) 277.

55 See GDPR art 5(2) and POPIA sec 8.

56 POPIA sec 4. For GDPR's principles, see art 5.

57 GDPR arts 6(1)(a)-(f) and POPIA secs 11(1)(a)-(f).

58 GDPR art 5(2).

59 GDPR art 5(1)(a).

60 GDPR art 5(1)(b).

61 GDPR art 5(1)(d).

the principles of 'data minimisation',[62] 'storage limitation'[63] and 'integrity and confidentiality'.[64]

Beginning with the first and broadest principle, ADM and profiling will be regarded as 'lawful' if the processing is predicated on one or more of the following grounds for lawful processing: (i) consent;[65] (ii) contractual obligations;[66] (iii) legal obligations;[67] (iv) vital interests of a data subject;[68] (v) public interest;[69] or (vi) the legitimate interests of a controller or those of a third party.[70]

As far as 'transparency' is concerned, it is regarded by the European Data Protection Board (EDPB) – previously the Article 29 Working Party (29WP) – as being at the core of GDPR[71] in that it is 'intrinsically linked to fairness'[72] and the principle of accountability. I concur with the EDPB in that the enforceability of all data subject rights require transparency between controllers and data subjects. That said, article 12 requires controllers to process 'transparently' by (i) communicating with data subjects in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language';[73] and (ii) facilitating the invocation of prong one rights by enabling and co-operating with data subject requests[74] – which must be undertaken free of charge, except where requests are unfounded or excessive.[75] Data subjects are afforded, among other rights, the right to (i) be notified about data collected from data subjects[76] or third parties,[77] and in such cases be provided with information to aid

62 GDPR art 5(1)(c).
63 GDPR art 5(1)(e).
64 GDPR art 5(1)(f).
65 GDPR art 6(1)(a).
66 GDPR art 6(1)(b).
67 GDPR art 6(1)(c).
68 GDPR art 6(1)(d).
69 GDPR art 6(1)(e).
70 GDPR art 6(1)(f).
71 *Guidelines* (n 18) 9.
72 Art 29 *Guidelines* (n 18) 5.
73 GDPR art 12(1).
74 GDPR arts 12(2), (3) & (4).
75 GDPR art 12(5).
76 GDPR art 13.
77 GDPR art 14.

transparency; (ii) access data;[78] (iii) rectify data;[79] (iv) erase data[80] ('the right to be forgotten'); (v) restrict the processing of data; and (vi) object to the processing of data.[81]

In respect of ADM and profiling, notification and access rights explicitly acknowledge these processes and require that data subjects either be notified[82] of, or have access[83] to 'the existence of automated decision-making, including profiling … and, at least in those cases, *meaningful information* about the *logic involved*, as well as the *significance* and the *envisaged consequences* of such processing for the data subject'.[84]

While this 'explanatory provision' may appear promising, ~~I note four limitations.~~ First, the obligation to notify data subjects about such processing in terms of article 13(1) is limited to 'the time when personal data are obtained'[85] and places no further obligation on a controller to inform a data subject *ex post*. At the time of notification, ADM or profiling may not have taken place, and in such cases it would be impossible to pre-emptively provide 'meaningful information' or 'envisaged consequences'. Also, data mining using ML algorithms is a 'highly dynamic process',[86] the logic of which evolves over time, thus making explanations very difficult, if not impossible.

Second, concerning information that is not obtained directly from data subjects (article 14), I emphasise that neither GDPR nor the WP29 guidelines[87] consider observations, inferences or knowledge discovered about a data subject through a data-mining process as an alternative source of personal data, and in turn, the notification requirements (towards data subjects) under article 14 do not apply. In a BD and AmI scenario, the most valuable information ('knowledge') relating to a data subject is not obtained directly from a data subject but rather through 'descriptive' and 'predictive' data mining.[88]

78 GDPR art 15.

79 GDPR art 16.

80 GDPR art 17.

81 GDPR art 21.

82 GDPR arts 13-14.

83 GDPR art 15.

84 GDPR arts 13(2)(f), 14(2)(g) & 15(1)(h) (my emphasis).

85 GDPR art 13(1).

86 Kamarinou and others (n 26) 4.

87 *Guidelines* (n 18) para 23.

88 BW Schermer 'The limits of privacy in automated profiling and data mining' (2011) 27 *Computer Law and Security Review* 46.

Third, regarding the right of access to information, article 15(1) sets out that data subjects have the right to obtain confirmation as to whether or not their personal data is being processed, as well as a copy thereof.[89] When read with the above 'explanatory provision', it appears that article 15 is the closest embodiment of a 'right to explanation' under the GDPR, in that unlike articles 13 to 14, it may be invoked *ex post* ADM or profiling processes. However, it is imperative to point out that this right of access is subject to article 15(4) which requires that any access to information does not 'adversely affect the rights and freedoms of others'.[90] In the context of a controller who utilises ADM or profiling as part of its business model, providing an explanation as to the 'logic involved' may be argued to impact on intellectual property or trade secrets of the controller. The fourth and final limitation relates to the semantics of the 'explanatory provision' and impacts on all of the aforementioned rights already described. That said, Wachter, Mittelstadt and Floridi argue that the semantics of the provision point to a right of explanation relating to 'system functionality, not the rationale and circumstances of specific decisions'[91] – the consequence being that there is no transparency about the reasons for specific decisions.

The second principle of 'purpose limitation' described by article 5(1)(b) not only requires that the collection of personal data be for 'specified', 'explicit' and 'legitimate' purposes, but that the further processing of personal data be principally limited to the initial purpose for which the data was initially collected.[92] Savin succinctly describes this principle as 'delegitimising secondary uses of data'.[93] This principle ought to be considered in light of the aforementioned 'data minimisation' and 'storage limitation' principles – which may be inherently difficult to reconcile for controllers engaged in ADM or profiling practices as 'data minimisation is inimical to the underlying thrust of BD'.[94] In this light, the right to object to the processing of personal data in cases of profiling is expressly limited to instances where a controller is lawfully processing a data subject's personal data on the grounds of either 'public interest'[95] or 'legitimate interests'.[96] In other words, where processing is based on consent or one of the other lawful grounds, a data subject cannot object but at most may withdraw

89 GDPR art 15(3).
90 GDPR art 15(4).
91 Wachter and others (n 35) 9.
92 GDPR art 5(1)(b).
93 Savin (n 29) 257.
94 Rubenstein (n 3) 78.
95 GDPR art 6(1)(e).
96 GDPR art 6(1)(f).

consent and cease utilising the controller's services – this imbalance of power is something to be monitored.

The third and last principle mentioned herein is that of accuracy. In the context of profiles (and decisions that are based on profiles), 'clean', accurate data is essential for data mining techniques – especially those 'predictive' in nature. Thus, where inaccurate profiles have been created, upon which inaccurate decisions have been made, it becomes vital that a data subject has the right to rectify,[97] erase[98] or restrict[99] such processing activities. Under GDPR, the right to rectification is unconditional, and the right to restriction of processing considers inaccuracy of data as a valid ground for restriction.[100] The right to erasure, however, does not contemplate profiling or inaccuracy as a ground for invocation of the right. Instead, it allows for erasure based on a successful objection by the data subject. Yet, as elucidated above, the right to object is narrowly drafted to only be applicable when processing is based on certain grounds and, therefore, this right does not serve as much utility as the right to rectify or restrict.

In concluding GDPR's first prong, it is noted that extra protections are provided to data subjects including the right to data portability.[101] Furthermore, the unique requirements of privacy by design[102] and data protection impact assessments where the 'systematic and extensive evaluation of personal aspects relating to natural persons'[103] takes place, are particularly reassuring – especially when viewed in conjunction with GDPR's requirement of 'prior consultation' (discussed more fully in part 4). Nevertheless, while being extensive, several aspects of GPDR's first prong have been shown to be limited in the context of ADM and profiling processes.

3.3.2 POPIA prong one

Whereas GDPR's first prong separates its processing principles, lawful grounds for processing and data subject rights (which receive a dedicated chapter), POPIA's first prong intertwines its lawful grounds for processing and data subject rights within its processing conditions. To aid comparison,

97 GDPR art 16.
98 GDPR art 17.
99 GDPR art 18.
100 GDPR art 18(1)(a).
101 GDPR art 20.
102 GDPR art 25.
103 GDPR art 35(3)(a).

I will therefore assess POPIA's first prong in a similar sequence to that of GDPR.

POPIA's eight conditions for lawful processing are listed in section 4 and all stem from the first principle of 'accountability'[104] which requires compliance with POPIA throughout the processing life cycle. In terms thereof, personal information must be collected for specified purposes[105] and processed in a limited,[106] open,[107] accessible,[108] (iv) accurate[109] and (vi) secure manner.[110]

Starting with the 'processing limitation' condition, processing will be lawful and justified if predicated on one or more of the following grounds: (i) consent;[111] (ii) contractual obligations;[112] (iii) legal obligations;[113] (iv) legitimate interests of a data subject;[114] (v) public law duties;[115] and/or (vi) the legitimate interests of a responsible party or of a third party.[116] Such processing must also be 'adequate, relevant and not excessive'[117] in terms of the 'minimality condition' – which ultimately runs contrary to the nature of data mining processes. Lastly, a right to object is also provided for, subject to the same limitations as those in GDPR, with the addition of an alternative grounds of processing ('legitimate interests of the data subject').[118]

Closely connected, POPIA's 'further processing limitation' goes on to provide that any further processing must be compatible with the purpose for which it was collected[119] and that when testing for compatibility, 'the

104 POPIA sec 8 (Condition 1).
105 POPIA secs 13-14 (Condition 3).
106 POPIA secs 9-12 (Condition 2) and POPIA sec 15 (Condition 4).
107 POPIA secs 17-18 (Condition 6).
108 POPIA secs 23-25 (Condition 8).
109 POPIA sec 16 (Condition 5).
110 POPIA secs 19-22 (Condition 7).
111 POPIA sec 11(1)(a).
112 POPIA sec 11(1)(b).
113 POPIA sec 11(1)(c).
114 POPIA sec 11(1)(d).
115 POPIA sec 11(1)(e).
116 POPIA sec 11(1)(f).
117 POPIA sec 10.
118 POPIA sec 11(1)(d).
119 POPIA sec 15(1).

consequences of the intended further processing for the data subject'[120] must be taken into account, thereby serving as a useful yardstick for responsible parties when undertaking ADM processes.

Under its 'openness' condition, POPIA, like GDPR, requires a transparent relationship between responsible parties and data subjects so as to ensure that data subjects can understand what their rights are, and when to invoke them. Interestingly the 'openness' condition also requires responsible parties to keep a record of all processing activities. However, where ADM or profiling involve de-identified information, this obligation would not be applicable due to limitations on the definition of 'personal information' already discussed. Moving on, under POPIA's first prong data subjects have the rights to (i) receive notification when personal information is collected from a data subject or a third party and what such processing entails;[121] (ii) access information;[122] (iii) correct and request the destruction or deletion of information;[123] and (iv) object[124] to the processing of personal information.

In respect of POPIA's notification, collection and access rights, I note the following. First, unlike GDPR's 'explanatory provision', a right of explanation regarding ADM or profiling processes is not provided for in POPIA's first prong. Instead, a right of explanation is considered within its second prong, which will be discussed below in part 3.3.4. Second, while at first glance POPIA's collection rights appear to go further than those within GDPR – by requiring that personal information be collected directly from data subjects[125] – POPIA nonetheless recedes. What I am pointing to here is POPIA's waiver provisions located within its aforesaid notification and collection rights. Thereunder, data subjects may consent to (i) the collection of personal information from another source and (ii) non-compliance by a responsible party with their notification duties prescribed in section 18.[126] In such cases there is the danger that data subjects may unknowingly waive their rights to the transparent collection and processing of their personal information, *ex post* the conclusion of a contract, privacy policy or other binding document regulating the responsible party-data subject relationship. Under this provision, the danger continues in that not only may responsible parties be allowed to

120 POPIA sec 15(2)(c).

121 POPIA sec 18.

122 POPIA sec 23.

123 POPIA sec 24.

124 POPIA secs 11(3) & 18(1)(h)(iv).

125 POPIA sec 12(1).

126 POPIA sec 18(4)(a).

indirectly source personally identifiable information, but when coupled together with a waiver of notification rights, responsible parties would legally be allowed to keep such collection and processing activities from a data subject, unless an access request is made. I therefore contend that these waiver provisions, with an emphasis on section 18(4)(a), may pose a risk to the liberties of data subjects, especially in the context of BD and AmI processes, and ought to be subject to constitutional scrutiny.

Insofar as POPIA's right of access is concerned, its use is severely limited. Apart from not providing for a right of explanation of ADM or profiling processes, a data subject may at best 'request from a responsible party the record or a description of the personal information about the data subject held by the responsible party'.[127] Moreover, in such cases a responsible party may raise a ground of refusal to such request in terms of the Promotion of Access to Information Act 2 of 2000.

Regarding the information quality (accuracy) condition, POPIA closely mirrors GDPR's rights to rectify,[128] erase[129] and restrict[130] processing. It also places an onus on responsible parties to ensure the accuracy of personal information by way of 'reasonably practicable steps'.[131] In an ADM or profiling context, it is not clear what would constitute 'reasonable steps' owing to the unpredictable nature of data mining processes.

Lastly, in regard to the retention of records, POPIA requires responsible parties to not retain personal information 'longer than is necessary for achieving the purpose for which the information was collected or subsequently processed'.[132] This safeguard nevertheless is subject to the exceptions following therefrom, allowing retention on the basis of consent, performance of contractual obligations or purposes reasonably required for the functioning or activities of a responsible party[133] – all of which may be raised by a responsible party engaged in ADM or profiling practices. It is interesting to highlight, however, that section 14(3) places an obligation on responsible parties to retain any personal information used in a decision-making process for a period of time as prescribed by a law, code of conduct or, where none exists, for a reasonable time that enables a data subject to request access to such record. I contend that on

127 POPIA sec 23(1)(a).
128 POPIA sec 24(1).
129 As above.
130 POPIA sec 14(6).
131 POPIA sec 16(1).
132 POPIA sec 14(1).
133 POPIA sec 14(1)(b).

the basis of this 'accountability mechanism', it is plausible that a data subject may request access to a profile that has not yet been de-identified, and which has been used in a decision-making process.

To conclude POPIA's prong one rights, it is reiterated that while they follow GDPR's prong one rights quite closely (and develop notable accountability mechanisms) there is a significant degree of room granted to responsible parties for non-compliance with their obligations on the basis of 'consent'.

3.3.3 GDPR prong two

In respect of GDPR's second prong, solely ADM, including profiling, is specifically addressed under GDPR article 22. In terms of article 22(1), data subjects are afforded the right 'not to be subject to a *decision* based *solely* on automated processing, *including profiling*, which produces *legal effects* concerning him or her or similarly *significantly affects* him or her'.[134]

At the outset of this analysis, it is imperative to note that the drafting of article 22(1) is notoriously ambiguous and has given rise to two significant interpretive questions, the answers to which ultimately shape the extent and adequacy of protection against unlawful ADM and profiling practices under GDPR. The first question relates to the nature of the right contained in article 22(1) and revolves around whether the right constitutes either an 'election' (data subjects may object to the processing and nullify the decision) or a 'prohibition' (an automatic ban is placed on article 22(1) decisions). The second question is whether, in the absence of decision making, profiling is regulated.

Beginning with the first question, the EPDB has taken the position that the right should be interpreted as a general prohibition on the basis that this interpretation is in alignment with the fundamental principles of GDPR and the fundamental human rights GDPR seeks to protect.[135] In taking this stance, it refers to Recital 71 which speaks of specific instances where the processing considered in article 22(1) 'should' be allowed – by inference, meaning that such processing, by default, is prohibited. The 'prohibition' interpretation has been assented to by Wachter and

134 GDPR art 22(1) (my emphasis).

135 *Guidelines* (n 18) 20.

others[136] as well as by Kaltheuner and Bietti.[137] Further, it was followed by 'Austria, Belgium, Germany, Finland, the Netherlands, Portugal, Sweden and Ireland'[138] under the DPD's similarly-constructed provision.[139] Meanwhile, others like Bygrave[140] and Savin[141] have opined that the right should be interpreted as an election to object to such processing. The 'election' interpretation was also followed by the United Kingdom under the DPD. In December 2023 EU jurisprudence finally offered a binding interpretation of article 22(1), wherein the Advocate General of the Court of Justice of the European Union (CJEU), in the *Schufa* case, held that "*[d]espite the terminology used, the application of Article 22(1) of the GDPR does not require the data subject to actively invoke the right*".[142] The CJEU went on to affirm this interpretation and clarified that the right in article 22(1) is indeed a prohibition against solely ADM.[143]

In approaching the second question, I will begin with Recital 71. Thereunder, the legislators suggest that automated processing – in terms of article 22(1) – 'includes "profiling" that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person'.[144] The Recital goes further to state that the term 'decision' referred to in article 22(1) 'may include a measure, evaluating personal aspects relating to him or her'.[145] Accordingly, Recital 71 considers a profile constructed by automated means as a decision in and of itself and, thus, suggests that article 22(1) caters for the creation of profiles. Conversely, Wachter and others, Mittelstadt and Floridi[146] as well as Kaltheuner and Bietti[147] have viewed article 22(1) as not considering profiling in the absence of decision making. Yet, notwithstanding academia's opposing

136 Wachter and others (n 35) 20.

137 F Kaltheuner & E Bietti 'Data is power: Towards additional guidance on automated-decision making and profiling in the GDPR' (2017) 2 *Journal of Information Rights, Policy and Practice* 11.

138 Wachter and others (n 35) 19.

139 See DPD art 15.

140 L Bygrave 'Automated profiling: Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 *Computer Law and Security Review* 17-24.

141 Savin (n 29) 257.

142 Opinion of Advocate General in *OQ v Land Hessen and Schufa Holding AG (as intervener)* 16 March 2023.

143 *OQ v Land Hessen and Schufa Holding AG (as intervener)* (C-634/21) 7 December 2023 para 52.

144 GDPR Recital 71.

145 As above.

146 Wachter and others (n 35) 20.

147 Kaltheuner & Bietti (n 138) 11.

views Recital 71 is now corroborated by recent developments in the *Schufa* case, where the CJEU held that if a profile serves a 'determining role' in a decision, that profile will constitute a decision in and of itself, even where the Controller who generated the profile is not the decision-maker.[148]

Building on the above, I postulate the following thoughts: First, if article 22(1) was intended to constitute an 'election to object', it is arguable that the drafters would have clearly incorporated ADM, including profiling, as an objectionable ground within the 'right to object' in article 21(1). Second, and from a different angle, one may argue that because 'profiling' is included as a ground of objection under article 21(1) – and ADM is not – the legislators intentionally separated the two processes, providing a right to object for profiling in article 21(1), and a prohibition for solely automated ADM (even if based on profiles) in article 22(1). Lastly, the 'suitable measures' (discussed below) that must be put in place to safeguard data subject rights and freedoms are only required when article 21(1) is not applicable. Accordingly, I contend that if article 21(1) was intended to constitute an 'election', then the drafters would have required the aforementioned 'suitable measures' to be put in place where a data subject fails to make an 'election'. The absence thereof suggests that there is no need for suitable measures in the first place as the conduct to which the safeguards would apply is already prohibited.

Moving on, the applicability of the provision is constrained in two respects. First, protection is only operative when all of the definitional elements as contained therein are present, those being that (i) the data subject must have been subjected to a decision; (ii) the decision must have been reached solely by automated processing; and (iii) the decision must have produced legal effects and/or must pose a risk of significantly affecting the data subject.[149] It should be noted that although GDPR defines neither 'legal effects' nor 'significant effect', the EDPB has published guidelines to assist in the interpretation thereof.[150] Therein it regards 'legal effects' as decisions that affect one's legal rights and has adopted a subjective approach to 'significant effect', which may place an onus on data subjects to prove significance.[151] I wish to emphasise that in the context of AmI, it is possible that numerous seemingly 'insignificant' effects, can accumulate into a significant effect (in the form of subtle manipulation or 'hacking'

148 *Scufa Holding* Case C-634/21, para 50. Judgment of the first chamber. https://curia.europa.eu/juris/liste.jsf?num=C-634/21 (accessed 1 December 2023).

149 GDPR art 22(1).

150 *Guidelines* (n 18).

151 *Guidelines* (n 18) 21.

as envisaged by Harari)[152] – a scenario that has not been acknowledged by the EDPB.

Second, article 22(1) only protects data subjects in the absence of article 22(2)(a)-(c) exceptions, namely, contractual obligations,[153] explicit consent[154] and authorisation under a '[European Union] or member state law to which the controller is subject'.[155] In the event that article 22(1) is not applicable, controllers ought to implement 'suitable measures' that may include providing data subjects with the rights to (i) obtain human intervention; (ii) express one's point of view; and (iii) contest the decision.[156] At this juncture I note that despite Recital 71 suggesting that safeguards 'should' include 'a right to explanation of the decision', this right has not been incorporated into article 22 as an operative provision and, consequently, data subjects will need to rely on article 15 – albeit being limited in application. Lastly, as far as special category personal data[157] is concerned in the aforesaid instance, such data may only be utilised if the data subject has given explicit consent[158] or the processing is 'necessary for reasons of substantial public interest'.[159]

In concluding GDPR's prong two rights, it is submitted that they lack definition and require judicial clarification to determine their exact nature and scope.

3.3.4 POPIA prong two

In respect of the second prong, ADM is specifically addressed under section 71 of POPIA titled 'Automated decision making'. In terms of section 71(1), data subjects

> may not be subject to a *decision* which results in *legal consequences* for him, her or it, or which *affects* him, her or it to a *substantial degree*, which is based *solely* on the basis of the automated processing of personal information *intended to provide a profile* of such person including his or her performance at work, or his,

152 Harari (n 1).
153 GDPR art 22(2)(a).
154 GDPR art 22(2)(b).
155 GDPR art 22(2)(c).
156 GDPR art 22(3).
157 GDPR art 9(1).
158 GDPR art 22(4) as read with art 9(2)(a).
159 GDPR art 22(4) as read with art 9(2)(g).

> her or its credit worthiness, reliability, location, health, personal preferences or conduct.[160]

Unlike the (now resolved) ambiguity surrounding the nature of GDPR's article 22(1), POPIA's prong two right is clearly prohibitive and need not require any further analysis. However, in as far as the scope of the right is concerned, there appears to be confusion among South African academia that stems from an inaccurate conceptualisation of the processes of ADM and profiling, resulting in misinterpretations of the law.

As was made clear in part 2, ADM and profiling are distinct processes that may overlap in practice – specifically when profiles are applied in the process of decision making. However, I also emphasised that profiles can serve other functions when re-applied in a data-mining process and are therefore not limited to being applied in the course of decision making. Saying that, Naude views the section 71(1) prohibition as 'relating to automated decision making (also known as profiling)'.[161] Similarly, Roos holds that 'automated decision making is sometimes also called profiling'.[162].I respectfully submit that the aforesaid academics have overlooked that these two processes are distinct.

A by-product of the above confusion is that section 71(1) is misinterpreted. In their book Burns and Burger-Smidt state that '[t]he South African legislature has been alert to the dangers of processing personal information for the purposes of profiling and has expressly prohibited processing for this purpose in section 71 of the POPI Act'.[163]

On a similar note, the authors have affirmed their stance by arguing, with reference to section 71(1), that 'the POPI Act expressly prohibits the creation of a profile on the basis of automated processing'.[164] Again, and with respect, I contend that Burns and Burger-Smidt are mistaken. I argue instead that the right does not apply to profiling *per se,* but rather to decisions reached on the basis of solely automated profiling. By implication, I am also arguing that decisions that are reached in the absence of the solely automated application of a 'profile' fall outside the

160 POPIA sec 71(1) (my emphasis).

161 A Naude 'Data protection in South Africa: The impact of the Protection of Personal Information Act and recent international developments unpublished LLM dissertation, University of Pretoria, 2014 55.

162 A Roos 'Data privacy law' in D van der Merwe, A Roos & T Pistorius (eds) *Information and communications technology law* (2016) 462.

163 Burns & Burger-Smidt (n 38) 329.

164 Burns & Burger-Smidt (n 38) 331.

ambit of protection provided for in section 71(1). A final (non-technical and purely semantical) point I will raise is that the wording throughout POPIA (in the section title, as well as in section 60(4)(a)(ii) in respect of codes of conduct) both merely refer to 'automated decision making' – thereby pointing at the drafters' intention to regulate ADM, and not profiling.

Having clarified the scope of section 71(1), I turn to the terms 'legal consequences' and 'substantial degree' that create a threshold within the right. These terms are not defined, and at the time of writing there are no regulations, opinions or guidelines published by the South African Information Regulator to assist in applying these thresholds. When providing guidance on these thresholds, I recommend that the Information Regulator considers the 'cumulative effect' of seemingly insignificant decisions (as described above).

In further limiting the right in section 71, section 71(2) provides exceptions in the case where the decision is (i) taken in light of the conclusion or execution of a contract, where a data subjects request in terms of a contract has been met;[165] or where (ii) 'governed by a law or code of conduct'.[166] In both the aforesaid instances, section 71(3) requires responsible parties to put 'appropriate measures' in place for data subjects. These measures should provide data subjects with an opportunity to make informed representations about a solely automated decision[167] by providing data subjects with 'sufficient information about the underlying logic of the automated processing of the information relating to him or her'.[168] Commendably, the foregoing measures constitute an undeniable right to explanation that has been shown to be absent under GDPR. Yet, critically, section 71 does not specify anything concerning instances where 'special personal information'[169] or information on children is used to make automated decisions.

In concluding POPIA's second prong, I reiterate that there is no scope for protection against unfair profiling practices and that decisions made in the absence of an applied profile have also been shown to be unregulated. POPIA's right of explanation, however, must be praised.

165 POPIA sec 71(2)(a)(i).

166 POPIA sec 71(2)(b).

167 POPIA sec 71(3)(a).

168 POPIA sec 71(3)(b).

169 POPIA sec 1.

4 Contextualising current regulation in an age of big data and ambient intelligence

4.1 Findings on extent

4.1.1 A deep-rooted lacuna

In part 3.2 I highlighted that the foundational definitions of 'personal data' and 'personal information' under GDPR and POPIA, respectively, indicate that the extent of protection is limited to information that is personally identifiable. This limitation is expressly confirmed in both laws.[170] Despite an attempt in GDPR to provide protection for de-identified personal data that is capable of being re-identified, I have contended that the provision is conflicted and lacking in enforceability. POPIA, on the other hand, simply does not provide protection in such instances. Consequently, I find that none of the rights discussed in part 3.3 above apply to de-identified personal information or group data. I draw attention to this limitation as a deep-rooted *lacuna* inherent not only in GDPR and POPIA, but in all data protection laws stemming from principles of the OECD Guidelines.[171]

4.1.2 Opacity of the transparency principle

In part 3.3 I described the rationale behind the processing conditions of 'transparency' and 'openness' as seeking to advance the informational self-determination of data subjects by enabling the enforcement of their rights when the processing of their data is unlawful, unfair or inaccurate. Yet, as Hildebrandt puts it, 'even if the law attributes such rights of transparency and the right to resist automated decision making, these rights remain paper dragons as long as we lack the means to become aware of being profiled'.[172]

In conjunction with the *lacuna* described above, I have found two catalysts that increase opacity between data subjects and responsible parties, ultimately rendering 'the exercise of data subject rights highly theoretical'.[173] On the one hand, the lack of recognition of data mining as an essential source for the collection of personal information is detrimental

170 In respect of GDPR, see Recital 26. In respect of POPIA, see sec 6(1)(b).

171 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, as amended on 11 July 2013.

172 Hildebrandt (n 4) 248.

173 B-J Koops 'The trouble with European data protection law' (2014) 4 *International Data Privacy Law* 252.

to transparency. Without notification, it is difficult, if not impossible, for data subjects to holistically gauge what new information is being mined, whether it is being de-identified, how it is being processed and what the consequences of such processing may be. On the other hand, in practice, responsible parties communicate – half-heartedly so – with data subjects via privacy notices and terms of use that describe instances where, and how, personal information is collected and processed. Therein, data subjects often consent to 'umbrella clauses' that widely describe the purposes of processing – often in the spirit of 'providing a service' – leaving room for further processing that in many instances cannot be described at the time of collection because '[responsible parties] do not (and cannot) know in advance what they may discover'.[174] It is welcoming to note, however, that since the inception of GDPR, EU supervisory authorities have adopted a strong stance[175] towards opaque processing activities, having fined Google LLC a record sum of €50 million on the basis of 'lack of transparency, inadequate information and lack of valid consent'.[176]

4.2 Assessing inadequacy

Evidently, GDPR and POPIA both suffer the same 'regulatory dilemma'[177] – their processing principles (while being broad) are idealistic in the face of ADM and profiling practices, today, and more so, in an era of AmI that will 'create new vulnerabilities and aggravate existing ones'.[178] Briefly stated, important legal and ethical issues[179] that will arise in an age of BD and AmI are (i) algorithmic errors; (ii) discrimination in decision making; (iii) the allocation of group profiles to individual data subjects (de-individualisation); (iv) loss of individual autonomy; and (v) information asymmetries between responsible parties and data subjects.

With this in mind, Hildebrandt and Koops maintain that in an age of AmI most profiling will be indirect, upon aggregated information relating to large groups of data subjects.[180] In such a case, GDPR and

174 Rubenstein (n 3) 78.

175 See, eg, Core Review 'Major GDPR Fine Tracker – An ongoing, always-up-to-date list of enforcement actions', https://www.coreview.com/blog/alpin-gdpr-fines-list/ (accessed 15 September 2020).

176 CNIL 'The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC', https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed 22 August 2020).

177 As above.

178 Hildebrandt & Koops (n 9) 433.

179 Hildebrandt & Koops (n 9) 434. See also Kamarinou and others (n 27) 46.

180 Hildebrandt & Koops (n 9) 434.

POPIA, as they stand, cannot be relied upon to protect data subjects from responsible parties who collect and apply new 'knowledge' that is mined from de-identified information. Moreover, as I alluded to above, the prong two rights of GDPR and POPIA are narrowly constructed to cater for instances where tangible, 'significant' or 'legal' effects on data subjects are observed. In an era of AmI, the ongoing, unobservable manipulation of what seem to be conscious thoughts, decisions and perceptions of data subjects may cumulatively result in significant effects that are unnoticeable in real time. This is what Zarsky refers to as 'the autonomy trap'.[181]

4.3 Forward-looking recommendations

It is undoubtable that GDPR and POPIA, in their current form, are inadequate insofar as ADM and profiling are concerned. Therefore, the following recommendations are made, each of which may be viewed in isolation, or in unison.

4.3.1 A shift from regulating 'collection' to 'usage'

The unfettered collection and processing of data on the basis of consent is not going to change, nor is the reliance of our digital society on BD data mining processes, the accuracy of which is reliant upon unconstrained masses of data.[182] On this basis, I am in agreement with Zarsky's assertion that the issues inherent in data mining may therefore best be addressed at the 'usage' stage as opposed to the 'collection stage' of data.[183] By focusing regulative efforts on 'how' data is being used in an ADM and profiling context, *sui generis* laws (highlighted below) may be developed to mitigate the shortcomings of current data protection law.

4.3.2 Sui generis laws

While the free flow of information is imperative in society and the economy of the twenty-first century and beyond, there will, in certain instances (such as those contemplated by prong two rights) be a need for 'constitutive laws' that enforce behaviour, as opposed to 'regulative laws' that aim to induce behaviour. Such 'future generation' data-protection laws have been proposed by Hildebrandt and take the form of (i) 'transparency

181 T Zarsky '"Mine your own business!" Making the case for the implications of the data mining of personal information in the forum of public opinion' (2003) 5 *Yale Journal of Law and Technology* 17.

182 T Zarsky 'Online privacy, tailoring, and persuasion' in KJ Strandburg & D Stan Raicu (eds) *Privacy and technologies of identity: A cross disciplinary conversation* (2006) 209-224.

183 T Zarsky 'Responding to the inevitable outcomes of profiling' in S Gutwirth, Y Poullet & P de Hert (eds) *Data protection in a profiled world* (2010) 61.

enhancing tools' (TET's),[184] especially in cases of group profiling; (ii) 'ambient law' – wherein legal norms are embedded into the technical architecture of systems[185] under a principle of 'transparency by design'; and (iii) laws specifically predicated on protecting data subjects against the unwanted application of profiles.

Additionally, I insist that policy makers and international data-ethics communities lobby for updated OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – last updated in 2013 – that may build upon Hildebrandt's propositions and provide 'a new generation of data protection rules, wherein the "identifiability" of the data subject is no longer a criterion'[186] and where principles are designed around ADM and profiling from the ground up. These updated Guidelines should be considered for interoperability with the OECD Principles on Artificial Intelligence,[187] which include principles relating to human intervention in artificial intelligence systems, as well as transparency around artificial intelligence systems, artificial intelligence-based outcomes, and decisions reached through the use of such systems.

4.3.3 External interventions

I posit two final recommendations involving data protection authorities in the EU, and the Information Regulator in South Africa ('supervisory authorities'). First, supervisory authorities ought to consider their statutory powers under 'prior consultation',[188] 'prior authorisation'[189] and 'codes of conduct'[190] provisions within GDPR and POPIA, respectively. When considering prior consultation/prior authorisation provisions, there may be scope for the enforcement of specific notification requirements in instances of potentially prejudicial profiling practices. In a South African context, section 57(2) of POPIA provides that the Regulator may, by law or regulation, require other types of information processing to be subject to prior authorisation 'if such processing carries a particular risk for the legitimate interests of the data subject'.[191] Furthermore, section 60 of POPIA empowers the Information Regulator to issue codes of conduct

184 M Hildebrandt 'Dawn of a critical transparency right for the profiling era' in J Bus and others (eds) *Digital enlightenment yearbook* (2012) 52-54.

185 Hildebrandt & Koops (n 9) 429.

186 Gutwirth & De Hert (n 17) 289.

187 OECD Principles on Artificial Intelligence (2020).

188 GDPR art 36.

189 POPIA sec 57(2).

190 POPIA sec 60(1) as read with sec 60(3)(c).

191 POPIA sec 57(2).

in various circumstances, including for 'any specified activity or class of activities'[192] which may include ADM and/or profiling.

Second, to rebalance information asymmetries, I propose the design and implementation of public databases, predicated on a right of access to information, wherein 'tools to access both data and profiles [relating to] data subjects'[193] are provided under the oversight of supervisory authorities and human rights watchdogs. Such a database could be populated with 'reported processing activities'. Within such a database, data subjects would be able to peruse all reported processing activities of responsible parties (or their operators) that are subject to the jurisdictional powers of a relevant supervisory authority. In this case, supervisory authorities may require any responsible party, who (i) processes personal information; (ii) engages in profiling; (iii) makes decisions based on personal information; or (iv) intends on further processing de-identified data, to report such processes. Unlike a 'right of explanation', such a system ought to be designed as a TET to assist data subjects in understanding, at a glance, which responsible parties are conducting profiling and what those profiles relate to, thereby allowing data subjects to invoke their prong one rights.

5 Conclusion

From semantic limitations and interpretive ambiguities, to deep-rooted *lacunae* and opaque transparency principles, an exploration of GDPR and POPIA (as jurisdictional yardsticks for global data-protection law) indicates that the protection of human liberties against proliferated ADM and profiling practices is inadequate in an age of BD and AmI. Instead of stretching these laws in their current form, specific, specialised legal and transparency-enhancing tools are required to rebalance information asymmetries between those who can 'see', and those who are being 'seen'. The protection of human self-determination has become, and will continue to be, increasingly prevalent. As Franklin D Roosevelt and many others have held, 'great power involves great responsibility'.[194] It is on this premise that solely automated decision-makers ought to be regulated.

192 POPIA sec 60(3)(c).

193 Hildebrandt & Gutwirth (n 17) 257.

194 FD Roosevelt 'Undelivered address prepared for Jefferson Day' (1945), http:// www.presidency.ucsb.edu/ws/?pid=16602 (accessed 20 September 2020).

References

Baratta, R 'Complexity of EU law in the domestic implementing process' (2014) 2 *TTPL* 293

Bibri, SE *The shaping of ambient intelligence and the internet of things* (Atlantis Press 2015)

Burns, Y & Burger-Smidt, A *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018)

Bygrave, L 'Automated profiling: Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 *Computer Law and Security Review* 17

Gutwirth, S & De Hert, P 'Regulating profiling in a democratic constitutional state' in Hildebrandt, M & Gutwirth, S *Profiling the European citizen: Cross-disciplinary perspectives* (Springer 2008) 288

Harari, YN *Homo Deus: A brief history of tomorrow* (Harper 2016)

M Hildebrandt 'Defining profiling: A new type of knowledge' in M Hildebrandt & S Gutwirth *Profiling the European citizen: Cross-disciplinary perspectives* (2008)

Hildebrandt, M & Gutwirth, S *Profiling the European citizen: Cross-disciplinary perspectives* (Springer 2008)

Hildebrandt, M & Koops, B-J 'The challenges of ambient law and legal protection in the profiling era' (2010) 73 *Modern Law Review* 3

Hildebrandt, M 'Dawn of a critical transparency right for the profiling era' in Bus, J and others (eds) *Digital Enlightenment Yearbook* (IOS Press 2012) 52

Hildebrandt, M 'Profiling and AmI' in Rannenberg, K, Royer, D & Deuker, A (eds) *The future of identity in the information society: Challenges and opportunities* (Springer 2009) 286

Hildebrandt, M 'Who is profiling who? Invisible invisibility' in Gutwirth, S and others (eds) *Reinventing data protection?* (Springer 2009) 239

Kaltheuner, F & Bietti, E 'Data is power: Towards additional guidance on automated-decision making and profiling in the GDPR' (2017) 2 *Journal of Information Rights, Policy and Practice* 11

Kamarinou, D, Millard, C & Singh, J 'Machine learning with personal data' in Leenes, R, Van Brakel, R & Gutwirth, S (eds) *Data protection and privacy: The age of intelligence machines* (Hart Publishing 2017) 97

Klimas, T & Vaiciukaite, J 'The law of recitals in European community legislation' (2008) 15 *ILSA Journal of International & Comparative Law* 61

Koops, B-J 'The trouble with European data protection law' (2014) 4 *International Data Privacy Law* 252

Mordini, E & Tzovaras, D (eds) *Second generation biometrics: The ethical, legal and social context* (Springer 2012)

Naude, A 'Data protection in South Africa: The impact of the Protection of Personal Information Act and recent international developments' unpublished LLM dissertation, University of Pretoria, 2014

Roos, A 'Data privacy law' in Van der Merwe D, Roos A & Pistorius, T (eds) *Information and communications technology law* (LexisNexis 2016) 462

Rubenstein, IS 'Big data: The end of privacy or a new beginning?' (2013) 3 *International Data Privacy Law* 2

Savin, A 'Profiling in the present and new EU data protection frameworks' in Nielsen, PA, Schmidt, PK & Dyppel Weber, K (eds) *Erhvervsretlige emne* (Djøf Forlag 2015) 253

Schermer, BW 'The limits of privacy in automated profiling and data mining' (2011) 27 *Computer Law and Security Review* 46

Wachter, S, Mittelstadt, B & Floridi, L 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2017) *International Data Privacy Law* 20

Wright, D, Gutwirth, S & Friedewald, M (eds) *Safeguards in a world of ambient intelligence* (Springer 2008)

Zarsky, T '"Mine your own business!" Making the case for the implications of the data mining of personal information in the forum of public opinion' (2003) 5 *Yale Journal of Law and Technology* 17

Zarsky, T 'Online privacy, tailoring, and persuasion' in Strandburg, KJ & Stan Raicu, D (eds) *Privacy and technologies of identity: A cross-disciplinary conversation* (Springer 2006) 209

Zarsky, T 'Responding to the inevitable outcomes of profiling' in Gutwirth, S, Poullet, Y & De Hert, P (eds) *Data protection in a profiled world* (Springer 2010) 61