5

African data protection laws and artificial intelligence – regulation, policy and ways forward*

Moritz Hennemann

Abstract

The chapter engages with the approaches to AI by the data protection laws in Africa, including at the level of regional economic communities (RECs) and the African Union (AU) level. It shall be evaluated if and to what extent respective approaches specifically regulate AI, and to what end. It is targeted at the question of whether specific patterns can be identified that might serve as an approximation to a unique African approach to AI and data protection. On this basis, the potential for specific (future) instruments will be considered.

1 Introduction

Artificial Intelligence (AI) is a regulatory challenge to societies worldwide. Regulators must decide on an adequate (legal) framework for the 'development' and usage of AI. This decision comes along with fundamental questions. The innovation potential and the associated risks for individuals, societies, and states have to be balanced out. Answers must also be provided to the question regarding to what extent one shall facilitate or restrict the usage of AI. This process can also be framed an a 'competition' between different regulatory instruments[1] – and there is obviously no 'right' solution, as different legal traditions, cultural settings, and societal values will necessitate different approaches.

[*] This chapter is based on a conference paper presented at the Centre for Human Rights, University of Pretoria's conference 'Privacy and data protection law and practice in Africa – Challenges and prospects'. I do thank my former academic research assistants, Dr Patricia Boshe and Ricarda von Meding, for their helpful preparatory research, their handling of the various (legislative) documents, and their critical thoughts and feedback along the way. This work was supported by the Bavarian State Ministry of Science and Culture. The manuscript was finalised in January 2021; later developments could not be considered.

[1] For details with respect to data protection law see M Hennemann 'Wettbewerb der Datenschutzrechtordnungen' (2020) 84 *Rabel Journal of Comparative and International Private Law* 864.

The term 'Artificial Intelligence' has been used in various contexts. In this chapter, AI refers to deploying algorithms that are not hierarchical programmed (pre-structured when-if-scenarios), but adaptable. Their (changing) parameters are not (even theoretically) fully foreseeable in advance – thereby, also their output (and the contexts in which those outputs might be of use) are not known and cannot be predicted beforehand. This process is also framed as 'self-learning.' Respective algorithms (constantly) derive patterns through processing non-personal and / or personal data. This is also to say that the identified patterns are 'path-dependent' on the used set of data – including the possibility that biases in the data spill over to the patterns identified. These algorithms are used in many scenarios and are labelled as 'weak' AI (non-existing 'strong' AI prerequisites some sort of 'consciousness' of the algorithm).

The technological realities of AI lead to numerous questions in different fields of law.[2] First and foremost, data laws are specifically relevant in this context. They form a significant regulatory instrument for AI as non-personal and/or personal data is the 'resource' for AI. While the processing of non-personal data is largely unregulated / left to contractual agreements, the processing of personal data triggers the domain of data protection law – which shall be the focus of this chapter. Data protection law is a legal field directed towards counterbalancing (potential) threats to personal data/privacy. However, it must be made clear from the outset that AI-based applications do not necessarily go along with a general threat to personal data/privacy. AI can also benefit privacy and data protection if respective applications are used exactly for privacy purposes (such as Personal Information Management Systems).

Nevertheless, at least traditional data protection regulation approaches do generally restrict the processing of personal data in the context of AI. Thereby, data protection regulation poses some basic challenges to AI – or to phrase it differently: there is specific tension between AI and data protection laws, for example, with regard to the data protection law principles of data minimisation and purpose limitation. These principles are, from the outset, at odds with the characteristics mentioned above of AI, especially the need for adequate data sets and unforeseeable outcomes. On this basis, for example, the European Union (EU) data protection law, the General Data Protection Regulation (GDPR), is strongly criticised in

[2] The Law Library of Congress 'Regulation of artificial intelligence in selected jurisdictions' (January 2019) gives an overview to general AI regulation in selected jurisdictions worldwide. For selected African jurisdictions see 119 ff (in parts), 129 ff; see also the comparative summary (including maps) by J Gesley at 1 ff. See eg with respect to competition law M Hennemann 'Artificial Intelligence and competition law' in T Wischmeyer & T Rademacher (eds) *Regulating Artificial Intelligence* (2020) 361.

significant parts of the literature.[3] The result is an ongoing debate about whether and to what extent specific (less strict or stricter) data protection rules with respect to AI should be implemented.

Against this background, this chapter will analyse the approach to AI by the current data protection laws in Africa, including at the level of Regional Economic Communities (RECs) and the African Union (AU) level.[4] It will first evaluate the extent to which respective approaches *specifically* regulate AI. On this basis, second, this chapter gives an overview of options for specific future instruments. This chapter does not engage the general application of African data protection laws to AI.[5]

2 African data protection laws and artificial intelligence: The current state

As a first step, this chapter gives an overview of the approaches to AI by the current (2020) African data protection laws, including at REC and the AU levels.

2.1 General overview

There seems to be no *AI-specific* data protection regulation in African states, at the AU[6] level or at the level of the RECs (as of 2020). The AU Digital Transformation Strategy for Africa, adopted in February 2020, acknowledges the lack of AI-specific regulation in Africa.[7] The 'Resolution on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in

[3] For details see Y Lev-Aretz & KJ Strandburg 'Privacy Regulation and Innovation Policy' (2020) 22 *Yale Journal of Law & Technology* 256; T Zarsky 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 *Seton Hall Law Review* 995.

[4] For a detailed introduction to the current state see G Greenleaf & B Cottier 'Comparing African data privacy laws: International, African and regional commitments' (2020) 32 *University of New South Wales Research Series* and P Boshe and others 'African data protection laws: Current regulatory approaches, policy initiatives, and the Way Forward' (2022) 3 *Global Privacy Law Review* 56.

[5] See in this regard the respective conference contributions / chapters in this book.

[6] See also Internet Society and Commission of the African Union 'Personal Data Protection Guidelines for Africa' (May 2018) https://iapp.org/media/pdf/resource_center/data_protection_guidelines_for_africa.pdf (accessed 01 October 2020), highlighting at 25 the need of policymakers to engage with: 'implications of emerging technologies (data mining, machine learning and Artificial Intelligence; autonomous systems; Internet of Things, etc.)'.

[7] African Union 'The Digital Transformation Strategy for Africa' (2020-2030) https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf (accessed 1 October 2020); see 43: 'Currently in Africa, emerging technologies are unregulated.'

Africa' (February 2021) of the African Union Commission points to the fact 'that while AI companies, as well as organisations and businesses that use AI technologies … have a significant impact on human rights protection in Africa, there is no comprehensive framework governing their operations to ensure that they comply with human rights obligations on the continent.'[8] It underlines 'the need for a comprehensive governance framework on AI technologies … in Africa in a way that enhances human rights protection on the African continent including protection of the ownership of data on individuals experience in the digital sphere'[9].

However, reviewing the situation through the lens of data protection laws in African states, the following point must be made from the outset: This is *not* to say that laws do not regulate AI in any manner. Data protection laws in Africa do exist and regulate the processing of personal data which also covers respective AI-based processes. The data processor is in this context inter alia bound by data protection principles, rules and limits set out by respective laws, especially data subject's rights. However, the identified legislation may be classified as general and *not AI-specific* data protection regulation. This does not mean African countries do not consider or test additional or complementary legislation and administrative structures.

2.2 Selected jurisdictions

The following section highlights the respective approaches taken in regards to data protection in the selected jurisdictions.[10] The section will refer to AI Strategies and legislation, but will not discuss constitutional rights to privacy in the respective countries.

[8] ACHPR/Res. 473 (EXT.OS/ XXXI) 2021, https://www.achpr.org/sessions/resolutions?id=504.

[9] As above.

[10] The following criteria led to the selection of specific jurisdictions: First, the following five jurisdictions were classified as the top five African jurisdictions in respect of 'Government AI Readiness' by the Oxford Insights and the International Development Research Centre in 2019 (Oxford Insights and the International Development Research Centre 'Government AI Readiness Index 2019' (2019) https://www.oxfordinsights.com/ai-readiness2019 (accessed 01 October 2020): Kenya (no 1 in Africa; no 52 globally), Tunisia (no 2 / no 54), Mauritius (no 3 / no 60), South Africa (no 4 / no 68), and Ghana (no 5 / no 75)). Second, the representation of RECs in different data protection frameworks in Africa (e. g. EAC, SADC, ECOWAS) was considered. Third, the enforcement especially by Mauritius of data protection laws and the awareness shown for data protection laws by, for example, the Ghanaian Data Protection Commission which organises by conferences and awareness programmes were considered.

2.2.1 AI strategies

There are various initiatives concerning AI at the strategic level in African states. Kenya, for example, has engaged with the usage of AI in different ways. In July 2019, the Kenya Ministry of Information, Communications and Technology published the report of the Distributed Ledgers Technology and Artificial Intelligence Taskforce 'Emerging Digital Technologies for Kenya – Exploration & Analysis' (Taskforce Report).[11] In April 2019, Kenya conducted the AI for Development Workshop as part of the AI Network of Excellence in Sub-Saharan Africa.[12] The Taskforce Report highlights the disruptive nature of AI, the potentials for the public and the private sector, and underlines the need to develop 'effective regulations to balance citizen protection and private sector innovation'.[13] The Taskforce Report explicitly refers to 'concerns about data privacy' as discussion points.[14] The Taskforce correctly highlights that 'AI may encourage the proliferation of surveillance states and digital totalitarianism. To fully optimise the benefits from AI, government data will be centralised, and such centralisation carries the risk that government could abuse its power and infringe on the privacy of its citizens.'[15]

Mauritius has handed down the AI Strategy of 2018[16] and the Digital Mauritius 2030 Strategic Plan[17]. The Strategy highlights (1) the usage of regulatory sandboxes for AI in order to *inter alia*, evaluate the adjustment to current legislation as well as the possibility of establishing an AI Council to monitor deployments and to develop new legislation, (2) a standing AI Committee on Ethics, and (3) governmental data centres.[18] The Strategic Plan also envisages the creation of the AI council and 're-engineering of user processes before [the] application of technology' and creation of an

[11] Kenya Ministry of Information, Communications and Technology (Distributed Ledgers Technology and Artificial Intelligence Taskforce) 'Emerging Digital Technologies for Kenya – Exploration & Analysis' (July 2019).

[12] Notes and videos of the workshop are available at: https://www.idrc.ca/en/news/workshop-launch-ai-network-excellence-sub-saharan-africa (accessed 01 October 2020).

[13] Kenya Ministry of Information, Communications and Technology (n 11) 9, 10, 39 et seq.

[14] Kenya Ministry of Information, Communications and Technology (n 11) 42.

[15] Kenya Ministry of Information, Communications and Technology (n 11) 43.

[16] Mauritius Artificial Intelligence Strategy: A Report of the Working Group on Artificial Intelligence (November 2018).

[17] Ministry of Technology, Communication and Innovation, Digital Mauritius 2030 Strategic Plan (2018).

[18] Mauritius Artificial Intelligence Strategy (n 16) at 3 et seq.

'enabling environment' for the management of big data.[19] The Strategic Plan additionally points to the fact that '[t]he Mauritian data protection and privacy law seeks as much as possible to balance [the] different concerns and interests, ideally in a way that does not unnecessarily hamper the scope for technological development.'[20]

South Africa has established a Presidential Commission on the Fourth Industrial Revolution (4IR)[21] that published an extensive report.[22] The report highlights regarding AI that an "ethical and transparent use of these new technologies" is of vital importance.[23] Pointing to data protection, the report proposes *inter alia* in-land data centres[24], a national open data strategy[25], a future '[f]ocus on data privacy and data protection laws and regulations'[26], and protection through 'South Africa's Information Regulator' to help 'South Africa meet international privacy standards'[27]. The report states that 'data management' should be placed 'at the cross-cutting base of the state and public-private partnerships'.[28]

2.2.2 Legislation

At the regulatory level, Kenya recently enacted the Data Protection Act of 2019[29] and the Computer Misuse and Cybercrimes Act of 2018.[30] The Kenya Data Protection Act does not *specifically* regulate AI, only the general rules of data processing (including automated decisions) apply (compare Sec. 4, 25, 30 and 35). The same is true for Mauritius (Data Protection Act of 2017),[31] South Africa (Protection of Personal

[19] Digital Mauritius 2030 Strategic Plan (n 17) 2, 6, 24, 32, 34 et seq.

[20] Digital Mauritius 2030 Strategic Plan (n 17) 36.

[21] Department of Telecommunication and Postal Services 'Notice 209 of 2019' *RSA Government Gazette* 42388.

[22] Dept. of Communications and Digital Technologies 'Report of the Presidential Commission on the 4th Industrial Revolution' *RSA Government Gazette 43834* (October 2020).

[23] Department of Communications and Digital Technologies (n 22) 149.

[24] Department of Communications and Digital Technologies (n 22) 300.

[25] Department of Communications and Digital Technologies (n 22) 302.

[26] Department of Communications and Digital Technologies (n 22)322.

[27] Department of Communications and Digital Technologies (n 22) 325.

[28] Department of Communications and Digital Technologies (n 22)138.

[29] Act 24 of 2019. See also AB Makulilo & P Boshe 'Data protection in Kenya' in Makulilo (ed) *African Data Privacy Laws* (2016) 317.

[30] Act 5 of 2018.

[31] Act 20 of 2017. See for details AB Makulilo 'The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius' (2021) 25 *The International Journal of Human Rights* 117; AB Makulilo 'Data protection of the Indian

Information Act of 2013,[32] Ghana (Data Protection Act of 2012),[33] and Tunisia (Data Protection Law in 2004).[34]

2.3 Summary

None of the aforementioned rules *specifically* regulate AI yet – despite different AI strategies pointing to that end. AI is (only) covered by the respective general rules on data processing in the respective states.

3 A comparative look at the European Union and the GDPR

The aforementioned national sets of norms generally follow the lines of the Data Protection Directive 1995 (DPD) and the GDPR. The European Union itself has no *AI-specific* data protection regulation. Although the GDPR was aimed at 'aligning' EU data protection law to modern technologies, article 22 GDPR, for example, only generally regulates 'automated individual decision-making.' This rule is complemented by article 13(2)(f) GDPR (identical article 14(2)(g) GDPR). The latter norm stipulates that 'the controller shall … provide the data subject with the following further information ... the existence of automated decision-making, including profiling, … 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.' Article 15(1)(h) of GDPR stipulates an additional right to obtain a confirmation on the existence of a respective automated decision-making. As it is true for the aforementioned pieces of regulation, the general GDPR rules for data processing apply.[35]

On the policy level, the European Commission published its communication on 'a European strategy for data' in February 2020.[36] The communication highlights the integral part the existing data

Ocean Islands: Mauritius, Seychelles, Madagascar' in Makulilo (n 29) at 277.

[32] Act 4 of 2013. See also A Roos 'Data Protection Law in South Africa' in Makulilo (n 29) at 189.

[33] Act 843 of 2012. See also DN Dagbanja 'The Right to Privacy and Data Protection in Ghana' in Makulilo (n 29) 229.

[34] Loi portant sur la protection des données à caractère personnel n° 2004-63 du 27 juillet 2004. See also AB Makulilo 'Data protection in North Africa: Tunisia and Morocco' in Makulilo (n 29) 27.

[35] See in this regard European Commission 'White Paper – On Artificial Intelligence – A European approach to excellence and trust' COM(2020) 65 final at 10.

[36] European Commission 'Communication – A European strategy for data' COM(2020) 66 final.

protection law plays for any future European regulation. However, it is possible that the EU might take steps to '[ensure] legal clarity in AI-based applications.'[37] The White Paper on AI states: '[S]ome specific features of AI (e.g., opacity) can make the application and enforcement of [the EU] legislation more difficult. For this reason, there is a need to examine whether current legislation can address the risks of AI and can be effectively enforced, whether amendments of the legislation are needed, or whether new legislation is needed. Given how fast AI is evolving, the regulatory framework must provide room for further developments. Any changes should be limited to clearly identified problems for which feasible solutions exist.'[38] The White Paper underlines the AI-related threats to data protection: 'By analysing large amounts of data and identifying links among them, AI may also be used to retrace and de-anonymise data about persons, creating new personal data protection risks even in respect to datasets that per se do not include personal data.'[39]

So, modifications of EU data protection law to regulate AI *specifically* are likely. For example, the European Commission underlines the need for transparency with respect to capabilities, limitations, and purposes. In addition, the Commission states: '[C]itizens should be clearly informed when they are interacting with an AI system and not a human being. … [A]dditional requirements may be called for to achieve the abovementioned objectives. If so, unnecessary burdens should be avoided. Therefore, no such information needs to be provided, for instance, in situations where it is immediately obvious to citizens that they are interacting with AI systems.'[40]

4 Balancing innovation and potential risks: The way forward

The Kenya Taskforce rightly concluded: 'Ultimately, the challenge for regulation is how to balance supporting innovation and competition while protecting customers, market integrity, financial stability and human life.'[41] To state the obvious, any AI-related regulation has to

[37] European Commission 'Artificial Intelligence' https://ec.europa.eu/digital-single-market/en/artificial-intelligence (accessed 01 October 2020).

[38] European Commission (n 35) 10.

[39] European Commission (n 35) 11. See also fn 34 herein: 'The [GDPR] and the ePrivacy Directive (new ePrivacy Regulation under negotiation) address these risks but there might be a need to examine whether AI systems pose additional risks. The Commission will be monitoring and assessing the application of the GDPR on a continuous basis.'

[40] European Commission (n 35) 20.

[41] Kenya Ministry of Information, Communications and Technology (n 11) 42.

strike a balance between threats and opportunities. Innovation should be possible, potential risks should be mitigated sensibly. On this basis, the potential for specific future instruments, may it be hard or soft law and at different levels, are considered. Furthermore, and specifically with respect to Africa, the African Union Commission correctly "[emphasises] the need for sufficient consideration of African norms, ethics, values, such as ubuntu, communitarian ethos, freedom from domination of one people by another, freedom from racial and other forms of discrimination in framing of global AI governance frameworks"[42].

4.1 General remarks on AI regulation

For any future regulation of AI, the regulatory model to be applied, whether on the national, the REC or the level of the African Union, has to be discussed.[43] Legislators will have to decide whether to change from the current '*one-size-fits-all'*-regulatory regime and to take the ostensibly more burdensome path of a sector-specific risk assessment which would then inform the approach to be taken. Regulatory sandboxes could also be used to test and evaluate specific types of regulation.[44] This comes along with a framework of accountability and parameters for an affirmation process for AI applications.[45] Obviously, further conditions to optimise the efficacy and to mitigate risks should be considered. A special focus on the quality of datasets as well as their regional relevance seems to be beneficial.[46] Technical methods coming close to anonymisation of data should be considered thoroughly.[47] Furthermore, an essential ingredient is that consumers have a general understanding of the data processing being undertaken and its general purpose.[48] This requires a consideration of how such an understanding can be achieved and is dependent on the extent to which duties to inform are an adequate tool to achieve this.

[42] ACHPR/Res. 473 (EXT.OS/ XXXI) 2021, https://www.achpr.org/sessions/resolutions?id=504.

[43] As above.

[44] Kenya Ministry of Information, Communications and Technology (n 11) at 11, 14; Report of the Presidential Commission on the 4th Industrial Revolution (n 22) at 324.

[45] R Calo 'Artificial intelligence policy: A primer and roadmap' 51 *U.C. Davis Law Review* 300 (2017); M Romanoff 'Building ethical AI approaches in the African context' *UN Global Pulse* 28 August 2019 https://www.unglobalpulse.org/2019/08/ethical-ai-approaches-in-the-african-context/ (accessed 01 October 2020).

[46] World Wide Web Foundation 'Artificial Intelligence – Starting the policy dialogue in Africa' (December 2017) at 7.

[47] C Dwork 'Differential Privacy' (2007), https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf; Calo (n 45).

[48] Romanoff (n 45).

Personal information management systems (see below) could be a viable alternative.

4.2 What kind of privacy?

Any regulation is dependent on the determination of the kind of privacy it seeks to protect.[49] It therefore can be asked whether regulators focus on individual privacy (or individual data protection) or on 'group privacy'.[50] Group privacy could either complement or substitute individual rights. Group privacy might be considered as a reflection of a community-orientated approach in data protection legislation, might be aligned to African norms, and especially to the socio-cultural principle of communalism popularly described as ubuntu[51] – as highlighted by the African Union Commission before and by Art. 8(2) of the Malabo Convention ('that any form of data processing … [recognises] the rights of local communities').

The future framework for individual data protection rights is linked to and dependent on the potential level of group privacy. On this basis, one might grant individual rights only on the basis of an AI sector-specific risk-based approach or in situations where processing of sensitive data takes place. In this regard, there should be an evaluation of the legal principles of traditional data protection laws principles, such as data minimisation and purpose limitation, as well as data subject's rights. For example, one could consider the shortcomings of the right to explanation (equivalent to Art. 13, 14, 15 GDPR), especially the usefulness of the respective explanation. Parameters of even simple algorithms tend to be too complex to explain in relation to everyday scenarios. Furthermore, with respect to the right not be subject to automated or autonomous decision-making (equivalent to Art. 22 GDPR), it should be borne in mind that a '*one-size-fits-all'* approach is likely to lead to an 'overblocking' of standard everyday

[49] See P Boshe in chapter one of this book.

[50] L Taylor and others (eds) *Group privacy: New challenges of data technologies* (2017); U Reviglio & R Alunge '"I am datafied because we are datafied": An ubuntu perspective on (relational) privacy' (2020) 33 *Philosophy & Technology* 595; M Christen & M Loi 'Two concepts of group privacy' (2020) 33 *Philosophy & Technology* 207; Romanoff (n 45).

[51] This refers to *Umuntu ngumuntu ngabantu abanye*, which can be translated as 'a person is a person through other persons'. There is a link between the concept of *ubuntu* and African philosophy emphasizing collectivist human relationships, see P Boshe 'Data Protection Legal Reforms in Africa' (2017) University of Passau PhD Thesis 64 fn 386 with further references as well as PD Rwelamila and others 'Tracing the African Project Failure Syndrome' (1999) 6 *Engineering, Construction and Architectural Management* 335 and AB Makulilo '"A Person is a Person through other Persons" A critical analysis of privacy and culture in Africa' (2016) 7 *Beijing Law Review* 192.

decisions and thus a sector-specific regulation or a regulation focused solely on the processing of sensitive data could be examined.

4.3 Societal data access

Any approach could go along with societal access to datasets. As long as respective data cannot be anonymised, the datasets might be used in defined circumstances to train AI applications, most likely on the basis of an open government approach.[52] The use of open government data for societal good could be fostered. The Digital Transformation Strategy also suggests this approach. The Strategy favours open data and the interoperability of data and data systems.[53] It proposes adopting open data standards and policies[54] and defining technology standards[55]. This is not to imply that the dataset has to be managed by the respective state. Governments could use a trusted intermediary which is supervised by various stakeholders, members of the civil society or regional or local communities – and accountable to them. In this respect, the Digital Transformation Strategy proposes 'a high-level Enterprise Information Service Architecture (EISA) … to promote and support inter-operability, open systems, … and best practices'[56].

4.4 Data security and technical standard-setting

Data protection is not complete without regulation on data security. Technical standards need to be set, particularly with respect to AI applications. Such standard setting should be based on a risk assessment to prevent the misuse of personal data, thereby fostering trust in the particular application. Therefore, standards for AI design processes should be developed that support general transparency and accountability, whether in the private or public sector.[57] Database-related standards should, alongside other factors, aim to minimise discriminatory biases.[58] Security-related, AI might even help to guarantee and to check the strength and standard

[52] World Wide Web Foundation (n 46) 7. See also Romanoff (n 45).

[53] The Digital Transformation Strategy (n 7) 3, 34

[54] The Digital Transformation Strategy (n 7) 3 & 22.

[55] The Digital Transformation Strategy (n 7) 30 & 33

[56] The Digital Transformation Strategy (n 7) at 29.

[57] Romanoff (n 45).

[58] Calo (n 45); Kenya Ministry of Information, Communications and Technology (n 11) 38, 43.

of data security.[59] In sectors with risky or sensitive data processing, the establishment of a certification structure should be considered. It has to be borne in mind that AI's 'self-learning' algorithms change and adapt. Any certification can only be a 'basic' test of the general structure, and not with respect to every 'outcome' of the algorithm. A certification structure could therefore entrust the certifying entities with monitoring duties.

The standard-setting and certification process does not need to be, and quite often cannot be, the exclusive remit of the state. Rather, entities or bodies might make use of external technical, legal, and political experts, either as committee members or as part of a public-private-partnership[60]. The participation and integration of further stakeholders (for example, civil society, open source-community) might be an additional trust-building option. In this direction, the Digital Transformation Strategy proposes the establishment of a 'framework on data policy and management for Africa'[61] and 'mechanism for regional cooperation and mutual assistance'.[62]

4.5 AI privacy-enhancing applications

Taking a step back, one might finally conclude that in tech-driven times, privacy relating to technical applications might only be reached by the very use of tech by the individual. Starting from Antitrust Law, the concept of an 'algorithmic consumer' (*Gal/Elkin-Koren*)[63] has made its way through other fields of law. The underlying premise is that individuals use technical applications, acting in their own interest. AI is not only used in relation to the individual but *by* the individual.[64] Respective applications are normally labelled as bots or autonomous agents. From a data protection law perspective, this refers to Personal Information Management Systems (PIMS).[65] These systems – at odds with traditional data protection laws – administer the personal data of the individual, act on the basis of the individual's general preferences of the individual, and value different offers on the market respectively. Individuals could thus have access to a

[59] E Segal 'The role of AI in data security' (19. July 2019) https://datafloq.com/read/role-of-ai-data-security/6616 (accessed 01 October 2020).

[60] Kenya Ministry of Information, Communications and Technology (n 11) at 11; Report of the Presidential Commission on the 4th Industrial Revolution (n 22) 138.

[61] The Digital Transformation Strategy (n 7) 47.

[62] As above.

[63] MS Gal & N Elkin-Koren 'Algorithmic consumers' (2017) 30 *Harvard Journal of Law & Technology* 309.

[64] Calo (n 45).

[65] https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en (accessed 01 October 2020).

broader variety of services, overcome potential lock-in-effects, and foster competition for privacy and privacy-protecting services.

4.6 AI model laws for Africa?

Next to hard law approaches, which might not be easy to agree on, a medium term-goal could also be soft law instruments fostering AI regulation ('AI model laws'); for example, drafted by the African Union or the African RECs.[66] Such model might also be based – if that is found to be a sensible solution – on an new approach giving ubuntu, communities, and group privacy a more appropriate place in legislation.[67] Such an approach might neatly fit into the broader policy framework. The Digital Transformation Strategy rightly points to the fact that especially for an envisioned African digital single market, '[b]eing prepared for digital transformation and emerging technologies such as Artificial Intelligence (AI) … is fundamental. Public policy, [l]egal and regulatory frameworks need to be up-to-date, flexible, incentive-based and market-driven to support digital transformation across sectors and across the continent regions.'[68] Policies should be 'designed based on a human-centred and holistic approach that also takes into account the local context and cross-cutting issues relevant to all stages of policy design and implementation.'[69]

5 Conclusion

There is yet no *AI-specific* data protection rules exist in African states as in the EU and on the REC and AU levels (as of 2020). AI is only regulated 'along the way' in data protection law, by the general rules applicable to data processing. On the basis of the aforementioned arguments, this current state is evaluated – especially where beneficial effects with respect to privacy and data protection are possible, for example, using personal information management systems. The adjustment of regulatory instruments should be considered. Ideally, legal traditions, different cultural settings, and diverse societal values will frame future African instruments (and beyond). To this end, this chapter proposes that lawmakers consider: (1) the non-use of mere 'copies' of the GDPR or the DPD[70]; (2) the integration of elements

[66] 'Toward a Network of Excellence in Artificial Intelligence for Development (AI4D) in sub-Saharan Africa' 3-5 April 2019. Such a model law would probably tackle not only questions of data protection law, but also other relevant fields of law.

[67] ACHPR/Res. 473 (EXT.OS/ XXXI) 2021, https://www.achpr.org/sessions/resolutions?id=504.

[68] The Digital Transformation Strategy (n 7) at 7.

[69] The Digital Transformation Strategy (n 7) 8.

[70] See generally Hennemann (n 1).

of 'group privacy'; (3) a risk-based approach for AI data protection law regulation; (4) enhancing the usage of AI, especially personal information management systems, by individuals; and (5) AI model laws at the REC or African Union level.

References

Boshe, P 'Data protection legal reforms in Africa' PhD thesis, University of Passau, 2017

Boshe, P and others 'African data protection laws: Current regulatory approaches, policy initiatives, and the way forward' (2022) 3 *Global Privacy Law Review* 56

Calo, R 'Artificial intelligence policy: A primer and roadmap' (2017) 51 *UC Davis Law Review* 399

Christen, M & Loi, M 'Two concepts of group privacy' (2019) 33 *Philosophy and Technology* 207

Dagbanja, DN 'The right to privacy and data protection in Ghana' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)

Dwork, C 'Differential privacy' (2007), https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf

Gal, MS & Elkin-Koren, N 'Algorithmic consumers' (2017) 30 *Harvard Journal of Law and Technology* 309

Greenleaf, G & Cottier, B 'Comparing African data privacy laws: International, African and regional commitments' *(2020) 32 University of New South Wales Research Series*

Hennemann, M 'Wettbewerb der Datenschutzrechtordnungen' (2020) 84 *Rabel Journal of Comparative and International Private Law* 864

Hennemann, M 'Artificial intelligence and competition law' in Wischmeyer, T and Rademacher, T (eds) *Regulating Artificial Intelligence* (Springer 2020)

Internet Society & Commission of the African Union 'Personal Data Protection Guidelines for Africa' (May 2018) https://iapp.org/media/pdf/resource_center/data_protection_guidelines_for_africa.pdf (accessed 1 October 2020)

Lev-Aretz, Y & Strandburg, KJ 'Privacy Regulation and Innovation Policy' (2020) 22 *Yale Journal of Law & Technology* 256

Makulilo, AB 'The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius' (2021) 25 *The International Journal of Human Rights* 117

Makulilo, AB '"A Person is a person through other persons" – A critical analysis of privacy and culture in Africa' (2016) 7 *Beijing Law Review* 192

Makulilo, AB 'Data protection in North Africa: Tunisia and Morocco' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)

Makulilo, AB 'Data protection of the Indian Ocean Islands: Mauritius, Seychelles, Madagasgar' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)

Makulilo, AB & Boshe, P 'Data protection in Kenya' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)

Rwelamila, PD and others 'Tracing the African project failure syndrome' (1999) 6 *Engineering, Construction and Architectural Management* 335

Reviglio, U & Alunge, R '"I am datafied because we are datafied"': An ubuntu perspective on (relational) privacy' (2020) 33 *Philosophy & Technology* 595

Romanoff, M 'Building ethical AI approaches in the African context' *UN Global Pulse* 28 August 2019 https://www.unglobalpulse.org/2019/08/ethical-ai-approaches-in-the-african-context/ (accessed 01 October 2020)

Roos, A 'Data protection law in South Africa' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)

Segal, E 'The role of AI in data security' (July 2019) https://datafloq.com/read/role-of-ai-data-security/6616 (accessed 1 October 2020)

Taylor, L and others (eds) *Group privacy: New challenges of data technologies* (Springer 2017)

Zarsky, T 'Incompatible: The GDPR in the age of big data' (2017) 47 *Seton Hall Law Review* 995