4

The ascent of artificial intelligence in Africa: Bridging innovation and data protection

Emmanuel Salami

Abstract

Artificial intelligence (AI) systems have transcended science fiction and are now globally used in almost every facet of human endeavour. Whether in the development of AI to perform defined tasks or in the actual performance of said tasks by AI, AI systems process large volumes of big data (which includes both personal and non-personal data) with vast consequences for the right to data protection. In certain cases, AI systems can collect (personal) data from unsuspecting data subjects, resulting in vast proportions of data processing that are not usually anticipated with traditional technological devices. This potentially raises a plethora of data protection law concerns. The acknowledgment of the potential implications of AI within and outside the scope of data protection law has led to a massive production of literature from regulators and scholars around the world aimed towards the regulation and lawful use of AI. However, it appears that the regulation of AI by data protection law has yet to attract such momentum across the African continent. This is despite the fact that there is evidence of wide usage of AI systems across the continent. This is further worsened by the lack of (sufficient) data protection regulatory instruments across many African countries. At the continental level, member states have failed to ratify the African Union Convention on Cybersecurity and Personal Data Protection, thereby making it impossible for it to come into force. The result of this can only be a violation of the right to data protection of the residents of African countries by both indigenous and foreign actors who ironically respect the rights of data subjects in countries and regions having sufficient data protection laws. AI promises to automate a lot of processes ensuring vast technological advancements in its wake. However, violations of the right to data protection owing to the lack or insufficiency of data protection regulatory instruments threatens to rob Africa of the benefits of AI. Relying on selected continental, regional and national data protection regulatory instruments, this chapter assesses the impact of the usage of AI systems on the right to data protection across the African continent. Data protection concerns that arise from the use of AI will be identified and assessed in light of these selected African laws with appropriate recommendations being made where necessary. The research methods that are

used to achieve the objectives of this chapter include a comparative analysis between certain aspects of the selected 'African' data protection laws under review and the data protection laws in some other countries and/or regions. The doctrinal research method is also relied upon by analysing existing statutory (where applicable), judicial and scholarly documents on the data protection regulation of AI in Africa. As there is a dearth of African literature on this topic, the overarching objective of this chapter is to spur discussions about the data protection concerns inherent in the use of AI across the African continent which, in turn, will birth more legislative interest, scholarly research and, hopefully, genuine efforts at regulation.

1 Introduction

The proliferation of artificial intelligence (AI) has become a global phenomenon partly because of the automation and relative ease it brings to the execution of various activities, especially those that could otherwise be very challenging. Notable industries across the African continent have adopted AI in their day-to-day operations. Africa has a fragmented regulatory approach to data protection law despite the enactment of the African Union Convention on Cybersecurity and Personal Data Protection (AU Convention)[1] which has been largely overlooked by most member states of the African Union (AU).[2] It would appear that the global rejuvenation of data protection law regulation that became the norm after the entry into force of the General Data Protection Regulation (GDPR)[3] has also had an impact across the continent with more African countries enacting data protection regulatory instruments after the entry into force of the GDPR.[4] In other cases, a good number of African countries have left

1 African Union Convention on Cyber-Security and Personal Data Protection (27 July 2014) EX.CL/846(XXV).

2 Only fifteen out of a total of 55 member states of the AU have ratified the convention. See African Union 'List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security And Personal Data Protection' https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (accessed 10 March 2024).

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (4 May 2016) OJ L119/1.

4 No less than eight African countries enacted data protection laws after the entry into force of the GDPR. These countries are Algeria (2018); Botswana (2018); Nigeria (2019); Uganda (2019); Kenya (2019); Congo-Brazzaville (Republic of Congo) (2019); Togo (2019); and Egypt (2020).

data protection law completely unregulated with varying consequences.[5] There is the possibility that data protection regulatory instruments across the African continent may not be well suited for the regulation of AI, thereby necessitating law reform. The importance of this consideration lies in the fact that the deployment of AI ordinarily poses enormous data protection law concerns, and this ought to be remediated.[6] It is arguable that limitations in technological advancements might have contributed to the selective lack of enthusiasm that bedevilled data protection law regulation across the continent.[7] Another school of thought might also blame the continent's chequered history with fundamental human rights enforcement as a reason for the hesitation that has courted its approach to the regulation of data protection governance.[8]

As previously stated, AI poses data protection concerns of vast proportions due to some of the following capabilities of AI: personal data[9] collection without the knowledge of data subjects; the collection of more personal data than ordinarily is necessary for the purpose of the processing activity;[10] making conclusions and decisions that affect the fundamental rights and freedoms of data subjects; and so forth. Therefore, any absence of proper regulation threatens to greatly violate the rights (including the right to dignity) of data subjects.[11] One of the objectives of this chapter is to consider the data protection concerns that are naturally attendant to the

5 At the time of writing this chapter, there are 18 African countries where data protection law is unregulated. See G Greenleaf & C Bertil 'Comparing African data privacy laws: International, African and regional commitments' (22 April 2020) University of New South Wales Law Research Series, https://ssrn.com/abstract=3582478 (accessed 15 September 2020).

6 Data subject means any identified or identifiable natural person that is the subject of personal data processing. See art 1 AU Convention; sec 2 Data Protection Act, 2019; Kenya Gazette Supplement 181 (Act 24) (DPAK); art 1 Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (adopted at the 37th session of the Authority of ECOWAS Heads of State and Government on 12 February 2010, Abuja, Nigeria) (ECOWAS Act).

7 Z Adaramola 'Why Africa is backward in technology – NOTAP' (21 June 2012), https://allafrica.com/stories/201206210900.html#:~:text=The%20National%20Office%20for%20Technology,growth%20of%20technology%20in%20Africa (accessed 14 September 2020).

8 Amnesty International 'Africa 2019' (Amnesty.org), https://www.amnesty.org/en/countries/africa/report-africa/ (accessed 10 September 2020).

9 Personal data means any information relating to an identified or identifiable natural person. Art 1 AU Convention; art 1 ECOWAS Act; sec 2 Data Protection Act of Kenya (DPAK).

10 Data processing is any operation carried out on personal data. See art 1 AU Convention; sec 2 DPAK.

11 European Union Agency for Fundamental Rights and the Council of Europe *Handbook on European data protection law* (2018) 19.

ascent of AI in Africa. The risks posed by these concerns are assessed in light of the efficacy of applicable data protection laws to mitigate identified risks. Since there is no uniform African data protection law, these concerns will be considered on the basis of selected continental, regional and national data protection laws. For this purpose, the AU Convention, the Economic Community of West African States Supplementary Act on the Protection of Personal Data (ECOWAS Act),[12] and the Data Protection Act of Kenya 2019 (DPAK) will be used to gauge the level of compliance across the continent.[13] These laws will collectively be referred to as the 'focus legislations'. The AU adopted the AU Convention in 2014 and it requires 15 signatories to come into force.[14] It got the fifteenth signature in April 2023.[15] In respect of the ECOWAS Act, the 15 member states of ECOWAS are bound by this Act and are obliged to adopt their own data protection laws.[16] In November 2019 Kenya passed its Data Protection Act into law making it the country's first data protection legislation.

Irrespective of the enforceability or effectiveness of these laws, they represent a selective overview of data protection law(s) across the continent and are considered herein for this purpose. This study considers these legislations because of their status as leading legislation at the continental, regional, and national levels. The Data Protection Act of Kenya has been particularly selected because of its adoption of internationally accepted data protection standards, making it a model African data protection legislation. The consideration of these regulatory instruments is limited to their role in achieving data protection compliance in the use of AI.

As far as possible, reference will only be made to actual deployments of AI across the African continent to ensure that the considerations herein are genuinely Afrocentric. This chapter is divided into six parts aimed at fully addressing relevant issues under consideration. Part 2

12 Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (adopted at the 37th session of the Authority of ECOWAS Heads of State and Government, 12 February 2010, Abuja, Nigeria).

13 Data Protection Act, 2019, Kenya Gazette Supplement 181 (Act 24).

14 Art 36 AU Convention.

15 Mauritania recent ratification made it the 15th ratification required to come into force. So far, only Angola, Cape Verde, Côte d'Ivoire, Congo, Ghana, Guinea, Mauritius, Mauritania, Mozambique Namibia, Niger, Rwanda, Senegal, Togo and Zambia have ratified the AU Convention. Thirteen other countries (Benin, Cameroon, Chad, Comoros, Congo-Brazzaville, Djibouti, Gambia, Guinea-Bissau, South Africa, Sierra Leone, Sao Tome & Principe, Sudan and Tunisia) have signed but not ratified it.

16 Arts 47 & 48 of the ECOWAS Act. See ECOWAS Revised Treaty of the Economic Community of West African States (ECOWAS) (24 July 1993). See also ECOWAS 'ECOWAS Law – Treaty', https://www.ecowas.int/ecowas-law/treaties/ (accessed 10 September 2020).

defines relevant concepts and terms such as AI, machine learning big data, and so forth. The instances of practical deployments of AI as well as the data protection concerns and applicable remediation actions in the use of AI in Africa are addressed in parts 3 and 4 respectively. Part 5 addresses the possible consequences of inadequate data protection legislations across the continent. This chapter concludes by assessing the above considerations and summarising the necessary steps for improving AI-specific data protection compliance in Africa. Some relevant concepts that are fundamental to this topic are subsequently considered.

2 An overview of relevant concepts

Although there is no consensus definition of AI, a perusal of scholarly literature would reveal some common conceptual attributes that cut across various definitions. This chapter will abstain from considering the definitional problems of AI and will rather focus on referencing some valuable definitions for the purpose of retaining a working definition for the purpose of this chapter. McCarthy, an AI pioneer credited with coining the term AI,[17] defined AI as the science and engineering of making intelligent machines, especially intelligent computer programmes. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.[18] Turing is another pioneer who designed what now is known as the Turing test used for determining the intelligence of machines.[19] According to Turing, a machine is to be considered intelligent if it could successfully pretend to be human to a knowledgeable observer.[20] Russel and Norvig define AI as 'the study of agents that exist in an environment and perceive and act'.[21] One common thread running through these definitions is the indication that AI systems are designed to simulate human intelligence even though, as McCarthy notes, machines can be trained by making them study 'problems the world presents to intelligence' rather than studying human beings.[22] AI can also be classified

17 P Stone and others 'Artificial intelligence and life In 2030: Report of the 2015-2016 Study Panel' (September 2016), https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf (accessed 10 September 2020).

18 J McCarthy 'What is artificial intelligence? (12 November 2007) 2-3, http://jmc.stanford.edu/articles/whatisai.html (accessed 10 September 2020).

19 AM Turing 'Computing machinery and intelligence' (1950) 433-460, https://www.csee.umbc.edu/courses/471/papers/turing.pdf (accessed 24 August 2020).

20 As above.

21 SJ Russell & P Norvig *Artificial intelligence: A modern approach* (2010) 7.

22 McCarthy (n 18) 2.

into strong AI[23] and weak AI.[24] As of today, weak AI is more prevalent as AI systems are mostly able to perform particular tasks with human input.

'Machine learning' is a type of AI that provides computers with the ability to learn without being explicitly programmed to perform relevant tasks.[25] Machine learning has also been defined as the use of algorithms[26] to analyse data with the aim of discovering useful patterns (relationships or correlations) that can be used to make inferences.[27] Machine learning is used to detect patterns in data in order to automate complex tasks or make predictions.[28] In lay terms, machine learning is used to detect patterns in data in order to automate complex tasks and/or make predictions. Another significant concept is 'big data' which is indispensable to the functioning of AI. This is partly because machine learning is only possible with the use of big data without which it will be impossible for AI to automate tasks or identify patterns. The term 'big data' is also not short of divergence in definition.[29] A widely-used definition of big data is '3Vs definition' which defines it as high volume, high velocity and high variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.[30] Based on this definition, it can be said that big data are large volumes of data that cannot be processed through the traditional methods of processing data. Having considered

23 Strong AI can perform unfamiliar tasks as it is equipped with comprehensive knowledge and cognitive capabilities ensuring that it has enough intelligence to solve problems. See I Bello 'Beginners' guide to artificial intelligence (AI)' (17 July 17 2017), https://becominghuman.ai/beginners-guide-to-artificial-intelligence-ai-ec8a409b6424 (accessed 13 October 2020).

24 Weak AI performs particular tasks with varying levels of human input. See Bello (n 23).

25 M Rouse 'What is machine learning', https://whatis.techtarget.com/definition/machine-learning-algorithm (accessed 24 August 2020).

26 An algorithm is an unambiguous procedure to solve a problem or a class of problems. It typically is composed of a set of instructions or rules that take some input data and return outputs. See C Castelluccia & D le Métayer nderstanding algorithmic decision-making: Opportunities and challenges' European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 624.261 (March 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf (accessed 7 September 2020).

27 S Finlay *Artificial intelligence and machine learning for business. A no-nonsense guide to data driven technologies* (2018) 6.

28 DE Sorkin 'Technical and legal approaches to unsolicited electronic mail' (2001) 35 *University of San Francisco Law Review* 325, 326.

29 See D Boyd & K Crawford 'Six provocations for big data' A decade in internet time: Symposium on the Dynamics of the Internet and Society, (September 2011) 1, https://ssrn.com/abstract=1926431 (accessed 6 September 2020).

30 Gartner IT glossary 'Big data', http:andandwww.gartner.comandit-glossaryandbig-data (accessed 7 September 2020).

the definition(s) of these relevant concepts, examples of the usage of AI in Africa are subsequently considered.

3 Actual deployments of artificial intelligence in Africa

A consideration of the actual deployment of AI in Africa aids the appreciation of the fact that AI now is an African reality that requires legislative attention and is not merely another academic discourse. This consideration will also aid an understanding of the concerns that might be posed by AI in the context of its application in Africa. Some existing deployments of AI across Africa are listed as follows:

AI system/Developer	**Industry**	**Processing activity**
Sophie Bot	Health care	This chatbot serves as a platform for young persons in Kenya to obtain information on sexual and reproductive health.[31]
SyeComp	Agriculture	SyeComp processes geospatial data from satellites and drone sensors for monitoring farms.[32]
DataProphet	Finance	DataProphet uses machine learning techniques for predictive analytics in conversation agents in South Africa.[33]

31 https://www.f6s.com/sophiebot (accessed 7 September 2020); C Harrington 'Improving access to sexual health education in Kenya with artificial intelligence' (15 January 2020) Humans of Machine Learning.

32 https://syecomp.com/ (accessed 7 September 2020).

33 https://dataprophet.com/de/ (accessed 7 September 2020).

Numberboost	Health care	Numberboost developed an AI system that supports mobile HIV clinics which provide medical access and services to different rural South African communities. Numberboost manages the scheduling and communication channels for patients seeking answers to sensitive medical questions.[34]
AI-based drones	Health care, product delivery, etc	AI-based drones are being used across the continent for various purposes which include the delivery of products to data subjects. In Rwanda for instance, drones are used to deliver critical medical supplies to hospitals and medical centers.[35]

34 https://www.numberboost.com/(accessed 7 September 2020).

35 JW Rosen 'Zipline's ambitious medical drone delivery in Africa' MIT Tech Review (8 June 2017), https://www.technologyreview.com/2017/06/08/151339/blood-from-the-sky-ziplines-ambitious-medical-drone-delivery-in-africa/ (accessed 7 September 2020).

Robots	Health care, service delivery, medical assistance, elder care, mining, etc.	Robots have been adopted in various African countries to provide support in various sectors of the African life and economy. A very popular example of this is the deployment of robots across the continent to provide support services at hospitals,[36] airports,[37] and universities,[38] as a response to the outbreak of the COVID-19 pandemic.

The deployment of AI across Africa is also visible in the finance sector where AI is being used for various purposes, including determining loan eligibility. There also is the opportunity for the futuristic deployment of autonomous cars in Africa even though as Africa's infrastructural reality suggests, this might not be happening any time soon.[39]

4 How do artificial intelligence systems collect (personal) data?

In order to enhance the comprehension of the relevant issues that are identified herein, it is important to identify some of the avenues through which AI collects (personal) data. AI systems typically collect large volumes of big data that which includes both personal and non-personal

36 D Miriri 'Rwandan medical workers deploy robots to minimise coronavirus risk' World Economic Forum (5 June 2020), https://www.weforum.org/agenda/2020/06/rwandan-medical-workers-robots-coronavirus-covid19-risk/ (accessed 7 September 2020).

37 A Odutola 'FG acquires profiling robots for airport' Nairametrics (27 June 2020), https://nairametrics.com/2020/06/27/fg-acquires-profiling-robots-at-airport/ (accessed 7 September 2020).

38 'Unilag gets robots for temperature, blood pressure checks' Vanguard (29 June 2020), https://www.vanguardngr.com/2020/06/covid-19-unilag-gets-robots-for-temperature-blood-pressure-checks-others/(accessed 7 September 2020).

39 S Malinga 'SA not ready for autonomous vehicles' ITWeb (7 October 2020), https://www.itweb.co.za/content/kYbe97XxPyQ7AWpG (accessed 7 September 2020).

data. It is the personal data collected by AI that forms the crux of this chapter. The data collection avenues identified in this part reflect some of the channels through which some of the AI systems stated above collect (personal) data. These avenues are identified in the paragraphs below.

One of the avenues for data collection in AI systems is through computer vision, which equips AI with the ability to 'see' and allows images or videos to be analysed using machine learning algorithms. Large volumes of (personal) data can be generated daily from AI systems using computer vision. These large volumes of (personal) data can be processed to provide insights capable of automating various systems and processes.[40] AI systems that are able to 'see' their environments, identify objects, scan documents, and so forth, are able to do this through the use of computer vision. In viewing its environment, AI systems designed with computer vision are able to capture large volumes of human images, buildings, vehicle plate numbers, and so forth, which, when combined with other data, might lead to the identification of natural persons. Computer vision has been used for a while in some popular applications, which include facial recognition, image classification, visual sensors, image search, photograph restoration, industrial robotics, autonomous vehicles, cancer detection, and so forth.[41] Computer vision uses specialised types of neural nets known as convolutional neural nets to build models of objects from a large collection of examples.[42]

AI collects large volumes of (personal) data collected through sensors that identify objects, persons, road users, and so forth. Most computer vision systems rely on image sensors. Some examples of sensors are lidar which uses lights to scan over a distance of 100 metres in all directions;[43] radar which uses radio waves to determine the speed, distance and angle of moving objects;[44] camera, which is the most popular sensor and is very effective for scene interpretation; ultrasound measures the distance between objects using sound waves. [45] Speech recognition technology is another avenue for data collection in AI. It allows users to interact with

40 J Tay and others 'Application of computer vision in the construction industry' (19 November 2019), https://ssrn.com/abstract=3487394 (accessed 7 September 2020).

41 N Malik & PV Singh 'Deep learning in computer vision: Methods, interpretation, causation and fairness', (28 May 2019), https://ssrn.com/abstract=3395476 (accessed 7 September 2020).

42 J Kaplan *Artificial intelligence: What everyone needs to know* (2016) 54.

43 A Herrmann, W Brenner & R Stadler *Autonomous driving: How the driverless revolution will change the world* (2018) 95.

44 Herrmann and others (n 44) 95-96.

45 As above.

AI by singling out their words or phrases in a specific language and thereafter converting it to a machine-readable format.[46] Mainstream usages of this technology can be found in Google Voice, Amazon's Alexa, Microsoft's Cortana, and Apple's Siri.[47] Other means of data collection include the use of data supplied into chatbots by its users, processing of anonymised[48] customer data for machine-learning purposes, and so forth.

5 Data protection concerns and remedies in the deployment of artificial intelligence in Africa

In the processing of large volumes of big data, AI systems also process the personal data of data subjects. The peculiarities of AI systems mean that said processing activities raise various concerns in the context of the right to data protection of data subjects. These concerns are assessed within the scope of the focus legislations with the aim of discovering how effective these laws are in resolving identified challenges. Recommendations aimed at the resolution of identified concerns are also considered. These concerns are identified as follows:

5.1 Lawfulness principle

The requirement that personal data should be processed lawfully embodies a foundational and fundamental principle of data protection law. This principle generally requires that the processing of personal data should be grounded in one of the recognised legal bases for processing personal data under data protection law.[49] This principle is reflected in the focus legislations as follows:

Article 13 (Principle 1) of the AU Convention provides, among others, that personal data shall be processed legitimately where data subjects have given their consent or also processed alternatively on the basis of a legal obligation; the performance of a task in the public interest or in the exercise of official authority vested in the controller or in a third party; for the performance of a contract to which the data subject is party or in order to

46 Kaplan (n 43) 57-60.

47 N van der Velde 'Speech recognition technology overview' Globalme Language and Technology (8 July 2019), https://www.globalme.net/blog/the-present-future-of-speech-recognition/ (accessed 7 September 2020).

48 Anonymised data is data that does not lead to the identification of natural persons because it has been deidentified and as a result does not fall within the scope of data protection law. See sec 2 DPAK.

49 Art 5 GDPR. See P Carey *Data protection: A practical guide to UK and EU law* (2018) 33. See also LA Bygrave 'Data protection law: Approaching its rationale, logic and limits' (2002) 10 *Information Law Series* 58.

take steps at the request of the data subject prior to entering into a contract; to protect the vital interests or fundamental rights and freedoms of the data subject. From this provision of the AU Convention, two apparent points come to mind: The AU Convention appears to make consent a primary legal basis, the use of which may only be derogated from where there are alternative legal bases that may be relied upon and 'legitimate interest of the controller' as a justifiable legal basis is omitted under said Convention.[50] Article 23 of the ECOWAS Act lists consent; compliance with a legal obligation; public interest of a public authority; performance of a contract or for the application of pre-contractual measures adopted at the data subject's request; for safeguarding the interests or rights and fundamental liberties of the data subject as legal bases for processing personal data. Section 25(b) of DPAK provides that personal data shall be processed lawfully, fairly and in a transparent manner in relation to any data subject. Section 30(1) of DPAK further provides that personal data shall only be processed on the basis of consent, the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; for compliance with any legal obligation to which the controller is subject; in order to protect the vital interests of the data subject or another natural person; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; the performance of any task carried out by a public authority; for the exercise of functions in the public interest; for the legitimate interests pursued by the data controller or other party to whom the data is disclosed and for the purpose of historical, statistical, journalistic, literature and art or scientific research.

One concern that pertains to the lawfulness principle is the determination of an appropriate legal basis for the processing activities of AI systems. In the use of AI, the most probable legal basis for conducting processing activities is the consent of the data subject or the performance of a contract. However, these can only be relied upon where personal data is collected from data subjects who are actively transacting with data controllers. The nature of AI systems that capture observed data,[51]

50 See art 6(1)(f) GDPR that provides for the use of 'legitimate interest of the controller' as a legal basis. The nature of this legal basis has been considered by the now defunct Article 29 Data Protection Working Party (A29WP). See A29WP Opinion 06/2014 on the 'Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' WP217 (9 April 2014).

51 Observed data is recorded automatically from data subjects even though they may be unaware of this in some cases. Interestingly, observed data can lead to the identification of other categories of personal data about a natural person. Eg, from a person's picture, their religious orientation (eg through the use of the hijab), race, political affiliations (through the inscriptions on clothing) etc might be deductible, thereby making observed data critical in the protection of personal data. For further readings on the

such as images of unsuspecting pedestrians and bystanders, renders the application of these legal bases legally impossible.[52] It suffices to say that innocent pedestrians and bystanders can neither be said to have consented to the collection of their personal data nor to have entered into a contract with data controllers. While 'legitimate interest' may appear like a possible legal basis, the balancing test that ought to be conducted before the said legal basis can be relied upon might suggest that the legitimate interest of the controller may not outweigh the fundamental rights and freedoms of data subjects, particularly pedestrians and passers-by who are unaware of any data collection.[53] Irrespective of this consideration, the use of legitimate interest as a legal basis will be inapplicable under the AU Convention as it is silent on said legal basis.

The nature of other possible legal bases, such as 'legal obligation', 'public interest' and 'vital interest', particularly in non-public sector processing activities, clearly makes these inapplicable in the context of this consideration.[54] Based on the above assessment, the focus legislations are not particularly suited for the processing of observed personal data.

To resolve this concern, it is necessary to revisit the data collection procedures of AI. The identified problems that may emanate from the lack of a sufficient legal basis for processing personal data may largely be avoided if data collection is directed only to data subjects that are transacting in one way or the other with data controllers. However, in some cases this recommendation may not always be feasible. For instance, in the use of autonomous cars, personal data, including IP addresses, images, and so forth, will be collected from both pedestrians and passers-by for reasons that include the prevention of accidents and mishaps.[55] Due to the fundamental purpose sought to be achieved by these processing activities, it might be necessary that laws be amended to define and justify

classification of data, see The Information Commissioner's Office 'Big data, artificial intelligence, machine learning and data protection' (4 September 2017) 12-13.

52 This very concern is related to the data minimisation principle and will be subsequently addressed.

53 For further readings on the necessity and nature of the 'balancing test', see Information Commissioner's Office 'Legitimate interest: At a glance', https:andandico.org.ukandfor-organisationsandguide-to-the-general-data-protection-regulation-gdprandlawful-basis-for-processingandlegitimate-interestsand (accessed 23 November 2018); Opinion of the Article 29 Working Party: Opinion 06/2014 on the notion of legitimate interests of the data Controller under Article 7 of Directive 95/6/EC.

54 For further readings on applicable legal bases for processing personal data, see Carey (n 50) 50-54.

55 L Sweeney 'Matching known patients to health records in Washington State data' (5 June 2013), https://ssrn.com/abstract=2289850 (accessed 26 September 2020).

these measures towards data collection, thereby making 'legal obligation' a justifiable legal basis for this purpose.[56] In some cases personal data might be anonymized, thereby making data protection law inapplicable. However, technological advancements mean that anonymised data may be reidentifiable in a way that leads to the identification of natural persons, thereby making personal data applicable.[57] Before personal data is treated as truly anonymised, adequate measures aimed at the prevention of data reidentification must be taken into consideration. Irrespective of the legal basis sought to be used in any processing activity, data subjects must be made fully aware of the ramifications of the processing activity especially because of the ability of AI to generate personal data from even the most innocuous of data categories.[58] This necessity of adequate information forms a key link to the transparency principle, which is addressed in the succeeding paragraph.

5.2 Transparent processing of personal data

Another principle of data protection that is relevant in the use of AI is the transparency principle that requires that data subjects should be provided with adequate information about the processing activity.[59] By virtue of this principle, data subjects should be provided with this right at the point of data collection. This principle is also important as it helps data subjects to pursue the enforcement of their data subject rights under any processing activity because the enforcement of such rights can only be achieved when data subjects are aware of the facts of the processing activity.[60] In practice, it is typical to provide data subjects with information about a processing activity through signposts, notice boards, privacy policies, and so forth.

56 E Salami 'Autonomous transport vehicles versus the principles of data protection law: Is compatibility really an impossibility?' (2020) *International Data Privacy Law Journal*, https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipaa017/6007987 (accessed 2 December 2020).

57 K Bode 'Researchers find "anonymised" data is even less anonymous than we thought' Motherboard (3 February 2020), https://www.vice.com/en_us/article/dygy8k/researchers-find-anonymised-data-is-even-less-anonymous-than-we-thought (accessed 26 August 2020).

58 Researchers have been able to identify the right driver from 15 minutes' worth of data from brake pedal use. See M Enev and others 'Automobile driver fingerprinting' (2016) (1) *Proceedings on Privacy Enhancing Technologies* 34-50, doi: https://doi.org/10.1515/popets-2015-0029.

59 Arts 5(1) and 13 GDPR. See Carey (n 49) 42. See also H Jackson 'Information provision obligations' in E Ustaran (ed) *European data protection law and practice* (2018) 169-193.

60 Art 29 Working Party Guidelines on transparency under Regulation 2016/679, adopted 29 November 2017, 17/EN WP260 rev.01, as last revised and adopted on 11 April 2018.

This principle is reflected in the focus legislations as follows: Article 13(5) of the AU Convention makes it mandatory for data controllers to disclose information on personal data. Article 27 of the ECOWAS Act requires data controllers to provide information about the processing of personal data. Section 25(b) of DPAK provides, among others, that data controllers and processors should process personal data transparently in relation to any data subject. The focus legislations are silent on what information is to be provided,[61] the manner in which the information is to be provided,[62] and at what point in the processing activity the information is to be provided to data subjects.[63] It is typical and rational to provide such information to data subjects before or at least at the time of data collection as this is will help them exercise their rights, for example, to object to the processing of their personal data. In the use of AI, the provision of data subjects with information about the processing activity when there is a subsisting processing activity with the data controller may not be a grave concern even though it remains to be seen if said information will be provided timeously, that is, before or at the time of personal data collection. In cases where observed personal data is collected from pedestrians and passers-by, this also poses concerns in the context of the transparency principle because of the difficulty of providing such information to data subjects. In some cases, particularly in the use of closed-circuit television (CCTV) cameras, video surveillance and facial recognition by law enforcement agents, it is typical to use signposts and notice boards to provide adequate information to the data subjects about the relevant processing activity. This method also provides data subject with information at the point of data collection. In an African context, some of the AI systems being developed are focused on providing rural dwellers with easy access to social services. Traditionally, African rural communities have established methods and channels of communication.[64] It might be a more effective approach if these established rural communication methods and channels for making relevant AI-related communications to rural dwellers are used where feasible. It is acknowledged that some of these methods and channels of communication might have become counterproductive in light of modern

61 Typically, data protection legislations specify information such as the name of the controller, name of the processor, retention periods, etc as some of the information that ought to be provided to data subjects. See art 13 GDPR.

62 See Recital 58 and art 12 GDPR. See also art 29 Working Party (n 60) 7-10.

63 Eg, art 13(1) of GDPR provides among others that data subjects are to be provided with information about their processing activity 'at the time when the personal data are obtained'. See also art 29 Working Party (n 60) 14-16.

64 Traditional media of communication as tools for effective rural development (iproject), https://iproject.com.ng/mass-communication/traditional-media-of-communication-as-tools-for-effective-rural-development-4257/index.html (accessed 22 September 2020).

technology. However, technologies that adopt the mode of communication of traditional systems might also be helpful if developed and adopted in rural communities. For instance, 'robot town criers',[65] fluent in the native language of the rural community and stationed at strategic places such as open markets, which can be programmed to disseminate information at strategic times, might be an effective way of providing rural dwellers with relevant information about the use of AI. This recommendation is even more effective for those communities lacking in electricity, connection to media houses, and so forth. Town hall meetings, sensitisations through media outfits such as radio and television stations, newspaper adverts, and so forth. may also be an effective means of providing relevant information. In the Google street view case of *EDÖB v Google* the Swiss Federal Supreme Court held (among other things) that in Google's collection of personal data, notice ought to be provided to data subjects in both the local and regional media.[66] To avoid selective application, it might be beneficial for regulators to specifically outline a minimum list of information that should be provided to data subjects in a processing activity.

5.3 Purpose limitation

In the processing of personal data, data controllers are required to specify and make the purpose of the processing activity explicit. This principle also requires that personal data should not be processed in a manner that is incompatible with the purpose for which they were initially collected.[67] This principle is reflected in the focus legislations as follows: Article 13(3)(a) of the AU Convention provides that data shall be collected for specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes. Article 25(1) of the ECOWAS Act provides that personal data shall be obtained for specified, explicit, and lawful purposes and shall not be further processed in any manner incompatible with such purposes. Section 25(c) of DPAK provides that personal data shall be collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes.

However, in the use of AI, machine learning generates new insights about data, which prompts data controllers to initiate new purposes for

65 Town criers serve as the traditional communication link between the village ruler(s) and the general village populace. See DSM Koroma 'Traditional forms of communication of the Malimba of Sierra Leone' (2018) 10, http://unimak.edu.sl/wordpress/wp-content/uploads/MALIMBA-PROF-KOROMA.pdf (accessed 22 September 2020).

66 BGE 138 II 346.

67 Art 5(1)(b) GDPR. See also Carey (n 49) 34; Bygrave (n 49) 61.

processing personal data a process known as data repurposing.[68] In such cases the legal basis and related considerations upon which the initial processing activity was carried out will not apply to the new processing activity because the processing activity did not form part of the purposes for processing personal data at the time of data collection.[69] However, it is clear that these provisions forbid further processing of personal data in a manner that is incompatible with the purposes for which it was initially collected. In practice, the provisions of the focus legislations are vague, particularly in the context of the provision restricting 'further processing of personal data in a manner that is incompatible with its initial purpose'. Therefore, the focus legislations are silent on the considerations necessary for the further data processing or repurposing of personal data in relation to the lawfulness principle. The factors to be considered in determining whether a new purpose of data processing incompatible with the initial purpose of processing are not outlined in the focus legislations and this could pose concerns in processing activities carried out by AI systems. This concern is even more amplified when the increased chances for data repurposing in AI systems are considered.

The regulatory approaches depicted in the relevant provisions of the focus legislations is distinguishable from article 6(4) of GDPR which provides, among others, conditions such as the relationship between the data controller and the data subject; the context of data collection; the possible consequences of increased processing on data subjects; and so forth. These conditions can then form the basis of an assessment for the purpose of revisiting the conditions for further processing in AI systems. Therefore, it is necessary for regulators to provide the necessary guidance which can help define the conditions that will justify further processing of personal data by AI systems. As the focus legislations are, there is much room for selective and subjective application of the rules for

68 AI processes large volumes of big data with a high tendency to discover new purposes of processing that were not envisaged at the commencement of the processing activity. For further readings, see R Pierce 'Machine learning for diagnosis and treatment: Gymnastics for the GDPR' (2018) 4 *EDPL* 339-340. See also M Shacklett 'Repurpose big data to get more analytics bang for your bucks' (28 January 2014), https://www.techrepublic.com/article/repurpose-big-data-to-get-more-analytics-bang-for-your-bucks/ (accessed 12 September 2020).

69 This principle can be further appreciated when one considers the fact that assuming a privacy impact assessment was carried out before the commencement of the processing activity, such privacy impact assessment will not have taken that new purpose into perspective, thereby exposing the processing activity to unforeseen risks.

further processing of personal data and this might potentially result in the violation of the right to data protection.

5.4 Algorithmic bias and decision-making artificial intelligence systems

Research has found that while the source of algorithmic bias[70] in AI systems may remain unclear, said algorithmic bias may have two prominent root causes. The first possible root cause emanates from the use of biased and non-representative training data at the machine-learning phase. The second possible root cause is the development of the algorithms behind relevant AI systems by biased and/or non-representative engineers.[71] Non-representative training data would be any data that does not truly represent all those that will be potentially subject to an AI system. Erroneous, unfair and unfounded inferences, predictions, conclusions, and decisions about data subjects are typically the end result of algorithmic bias. Once algorithms are biased, AI-based decisions are usually discriminatory and prejudicial against the group of people (typically minorities) who are underrepresented in the training data, thereby negatively affecting their fundamental rights and freedoms. Article 28 of the African Charter on Human and Peoples' Rights (African Charter) expressly forbids discrimination of any form by providing that 'every individual shall respect and consider other persons without discrimination, and to maintain relations aimed at promoting, safeguarding and reinforcing mutual respect and tolerance'.[72]

Evidence of discrimination is when data subjects suffer adverse treatments not justified by their performance.[73] As a continent, Africa is made up of divergent ethnic groups, nationalities and heterogenous people cohabiting across the continent. This means that distinct cultures, languages,[74] skin colour,[75] and so forth, form some of the characterisations

70 Algorithmic bias has been defined as the situation where machine learning programs inherit social patterns reflected in their training data without any directed effort by programmers to include such biases. See G Johnson, 'Algorithmic bias: on the implicit biases of social technology' (2020) 1-21 Synthese https://philpapers.org/rec/JOHABO-5 (accessed 14/09/2021).

71 B Cowgill and others 'Biased programmers? Or biased data? A field experiment in operationalising AI ethics' in Proceedings of the 21st ACM Conference on Economics and Computation (1 June 2020) 2, 22-23, https://ssrn.com/abstract=3615404 (accessed 16 September 2020).

72 Organisation of African Unity (OAU) African Charter on Human and Peoples' Rights (African Charter) 27 June 1981, CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982).

73 Cowgill and others (n 71) 3.

74 This might be relevant for voice recognition technology.

75 This might be relevant for facial recognition technology.

of Africans. For instance, it has been found in some cases that AI has failed to recognize or has erroneously recognised persons from minority races largely due to the use of non-representative training data and engineers at the machine-learning phase of the AI system.[76] Hypothetically, if non-representative data/engineers is used in an African context, AI systems developed by engineers of West African descent may not identify North Africans and *vice versa*. This is because said AI would have been trained with data that accommodates the physical features of certain tribes/ethnic groups to the detriment of others. Therefore, AI systems that will effectively and unbiasedly serve the African populace must employ data that is representative of the divergent ethnic groups, nations and people that make up the continent. Engineers must also be from divergent descent and/or must take the ethnic divergence of the continent into consideration when developing AI. In resolving this concern, it is necessary that representative training data that reflects all ethnic groups are used.[77] An equality impact assessment (EIA) aimed at identifying and remediating bias and inequity in AI systems before they are released for public use could also be helpful in mitigating identified biases.[78] To develop such an EIA, the input of stakeholders across the production lifecycle of the AI industry will be necessary to ensure that a truly representative and effective assessment is developed.

AI systems are able to make automated decisions that affect the fundamental rights and freedoms of data subjects thereby constituting a data protection law concern. AI algorithms can be trained to assess the personal data of data subjects and determine their eligibility in various scenarios, such as obtaining loans and mortgages.[79] AI is also being used to determine the rate of recidivism for convicted persons with such AI being the basis for deciding whether persons accused of certain crimes will be eligible for parole[80] or will be forced to serve out the full length of their

76 A Harmon 'As cameras track Detroit's residents, a debate ensues over racial bias' *The New York Times* 18 July 2019, https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html (accessed 14 September 2020). -recognition-

77 Cowgill and others (n 71) 2.

78 For further readings, see Biotechnology and Biological Sciences Research Council 'Equality impact assessment guidance and template', https://bbsrc.ukri.org/documents/equality-impact-assessment-guidance-template-pdf/ (accessed 14 September 2020).

79 D Faggella 'Artificial intelligence applications for lending and loan management' Emerj (3 April 2020), https://emerj.com/ai-sector-overviews/artificial-intelligence-applications-lending-loan-management/(accessed 17 September 2020).

80 NL Hillman 'The use of artificial intelligence in gauging the risk of recidivism' ABA (1 January 2019), https://www.americanbar.org/groups/judicial/publications/judges_journal/2019/winter/the-use-artificial-intelligence-gauging-risk-recidivism/ (accessed 7 September 2020).

sentence,[81] and so forth. If not properly managed, this can significantly affect the fundamental rights and freedoms of data subjects. In respect of automated decision making, the focus legislations contain the following provisions:

> Article 14(5) of the AU Convention provides that 'a person shall not be subject to a decision which produces legal effects concerning him/her or significantly affects him/her to a substantial degree, and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her'. Article 35(2) of the ECOWAS Act provides that 'no decision that has legal effect on an individual shall be based solely on processing by automatic means of personal data for the purpose of defining the profile of the subject or evaluating certain aspects of their personality'. Section 35(1) of DPAK provides that 'every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting the data subject'. Section 35(3) of DPAK provides that data controllers or data processors must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; the data subject may, after a reasonable period of receipt of the notification, request the data controller or data processor to reconsider the decision, or take a new decision that is not based solely on automated processing. Based on the provision of section 35(4) of DPAK, once the data controller or data processor receives the data subject's request in accordance with section 35(3) DPAK, they are to consider and/or comply with the request and inform data subjects of the steps taken to comply with the request.

It would appear that the focus legislations fall short of the requirements needed for attaining data protection compliance in automated decision making. These legislations forbid decisions made solely by automated means where such decisions affect the rights and freedoms of data subjects. From the provisions of these laws, it would appear that automated decisions will be lawful where they are not the sole basis for making a decision. This could be the case where an automated decision is made subject to the oversight or review of a human person. The DPAK is more elaborate and goes further than the other two focus legislations. Data controllers and data processors are mandated to notify data subjects about decisions based solely on automated processing and the data subjects can request a review of the decision or taking a new decision that is not based solely on

81 K Hao 'AI is sending people to jail and getting it wrong' MIT Technology Review (21 January 2019), https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/ (accessed 7 September 2020). For further readings on the use of AI in law enforcement, see AG Ferguson *The rise of big data policing: Surveillance, race, and the future of law enforcement* (2017).

automated processing. However, it still falls short of effectively protecting the rights of data subjects. The non-completeness of these provisions might result in some confusion in its interpretation. Some other standard features in the regulation of automated decision making are the rights of data subjects to obtain human intervention and review of automated decisions, to obtain an explanation, express their points of view and to contest automated decisions.[82] The focus legislations are either silent or contain sparse provisions on some of the standard provisions in the data protection regulation of automated decisions. The approach of data protection law is to generally ensure that the principles of data protection in non-automated personal data processing and decision making are also achievable in non-automated personal data processing and decision-making activities.[83] The right to an explanation of algorithmic decisions is also understood to be a necessary right of data subjects in automated decision making, which is linked to the requirement that personal data should be processed in a transparent manner.[84] Possible considerations to achieve explainability by design have been said to include 'relying on an algorithmic technique which meets the intelligibility requirements sufficient to provide data subjects with relevant explanation(s) or enhancing an accurate algorithm with explanation facilities so that it can generate an intelligible explanation for its results'. Human intervention and review of automated decisions before said decisions are adopted are also very necessary as they help reduce the violations of the right to dignity of the human person that automated decisions pose.[85] Human review can also reduce or prevent any bias or discrimination that might result from the use of non-representative training data or engineers.

82 These provisions are reflected in Recital 71 and art 22 GDPR.

83 The right to the explanation of automated decision making is seen as an extension of the accountability and transparency principle. S Wachter, B Mittelstadt & L Floridi 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation' (28 December 2016) 1, https://ssrn.com/abstract=2903469 (accessed 15 September 2020).

84 Wachter and others (n 83) 1, 4, 6.

85 Automated decision making affects the right to dignity of the human person because human beings might tend to trust automated decisions reached against them, thereby preventing the independent assessment of said decisions even when incorrect. For further reasons, see LA Bygrave 'Article 22. Automated individual decision-making, including profiling' in C Kuner, LA Bygrave & C Docksey *The EU General Data Protection Regulation (GDPR): A commentary* (2020) 526-528.

5.5 Data minimisation

AI systems are very prone to collecting more personal data than necessary for any processing activity.[86] This is partly because of the use of a substantial number of sensors and cameras that capture multiple categories of personal data. This principle requires that only data that is adequate, relevant and limited to what is necessary for the processing activity should be processed.[87] This principle does not require the reduction of data collection to an absolute minimum, but rather seeks to reduce data collection to the lowest possible level in relation to the purpose of processing.[88] The principle is reflected in article 13(3) (b) of the AU Convention, article 25(2) of the ECOWAS Act, and section 25(d) of DPAK. A possible example of the violation of this principle can be seen in the use of AI-based drones or other AI systems using cameras. If not properly managed, these drones will capture peoples' faces, homes, vehicle plate numbers and other categories of personal data capable of identifying natural persons with the effect being unlawful processing of personal data. If the data minimisation principle is to be reflected in AI systems, it is necessary for privacy by design[89] to be introduced early at the development phase of relevant AI systems. This will ensure that best practices that can prevent the capturing of unnecessary personal data can be introduced into AI systems at its development stage. For instance, where AI must capture human faces, the use of silhouettes that make human faces unidentifiable can be used once said faces are captured.

5.6 Accountability

The accountability principle requires that data controllers should be able to comply with the principles of data protection law.[90] Compliance with this principle would typically mean that data controllers have to document the rationale, principles and justifications that underlie their decisions. The focus legislations are silent on the accountability principle, which is not

86 C Melendez 'Data is the lifeblood of AI, but how do you collect it?' Infoworld (8 August 2018), https://www.infoworld.com/article/3296044/data-is-the-lifeblood-of-ai-but-how-do-you-collect-it.html (accessed 15 September 2020).

87 See art 5(1)(c) GDPR.

88 P Voigt & A von dem Bussche *The EU General Data Protection Regulation (GDPR): A practical guide* (2017) 90-91.

89 TJ Shaw *DPO handbook: Data protection officers under the GDPR, IAPP* (2018) 130-135.

90 For further readings on the accountability principle, see L Urquhart & J Chen 'On the principle of accountability: Challenges for smart homes and cybersecurity (17 June 2020); A Crabtree, R Mortier & H Haddadi 'Privacy by design for the internet of things: Building accountability and security' (13 July 2020), https://ssrn.com/abstract=3629119 (accessed 15 September 2020).

good for the overall data protection law compliance of AI systems.[91] This principle will be particularly essential to the data protection compliance of AI systems because of the non-regulation of various matters of data protection law compliance. The requirement to be able to demonstrate compliance with relevant data protection laws will put data controllers in a position where they are bound to ensure that they remain compliant with minimum thresholds of data protection law compliance for the fear that these decisions can be holistically reviewed by regulators in future. The fear of being sanctioned and/or fined based on documented information can motivate data controllers to strive towards compliance.

At the rate at which AI is growing on the continent, it is necessary for African countries to invest in the education of Africans on the legal (including data protection law) consequences of AI systems. This will serve the dual function of educating data controllers about measures to take towards compliance with relevant laws while data subjects will also be better educated about their rights and will pursue its enforcement as a result. Privacy impact assessments (PIAs) and privacy by design are two critical measures that will help identify data protection risks and introduce data protection law principles into AI systems at the very inception of the processing activity respectively. In the absence of adequate data protection laws, ethics will become very important to data protection law regulation. An appeal to the adoption of ethics in the regulation of data protection (in AI systems) is tantamount to an appeal to the moral compass of data controllers/processors to comply with minimum principles of data protection law because it is the right thing to do.[92] The problem with this approach is that data controllers/processors might not be very motivated to follow minimum standards for data protection compliance for reasons that include the lack of oversight. In such a scenario, one cannot help but wonder 'who will guard the guards?' The tendency might be for data controllers/processors to adopt the standards of compliance that favour them at any given time, thereby creating selective compliance with data protection principles. Despite its shortcomings, ethics could still be helpful in attaining some minimum level of compliance especially in regions with dormant law makers. Data protection ethics can be implemented into AI systems through sectoral regulatory bodies that will seek to protect the rights of data subjects by holding data controllers/processors accountable. For instance, respective medical associations can regulate data protection

91 Only DPAK contains selective applications of the accountability principle for specific processing activities. See secs 31(2)(d), 36, 49(2) & 52(2) of DPAK.

92 L Floridi & M Taddeo 'What is data ethics?' Oxford Internet Institute (2016) 5. See also K O'Keefe & D O Brien *Ethical data and information management* (2018) 39-49.

concerns in AI systems being used in medical practice by setting guidelines for protecting personal data.

Identified concerns	AU convention	ECOWAS Act	DPAK
Legal basis			
Transparent data processing			
Purpose limitation			
Algorithmic bias			
Algorithmic decision making			
Data minimisation			
Accountability			

The table above summarises the level of compliance of AI with selected requirements of data protection law. The 'red' circles represent complete non-compliance under the focus legislations; the 'yellow' circles represent those requirements that are partially compliant under the focus legislations. 'Green' circles would have represented those requirements that are compliant under the focus legislations. Unfortunately, none of the requirements can be said to be fully compliant. This shows that the usage of AI in Africa is not compliant and warrants more work if compliance is to be achieved.

6 Some implications of inadequate data protection law regulations for artificial intelligence systems

The inadequacy or non-existence of adequate AI-related considerations in data protection regulatory instruments poses risks not only to the rights of data subjects but also to the acceptance of AI as a legitimate member of our mainstream society. Some of these attendant risks that could emanate

from the use of AI underlie the suspicions that surround AI generally.[93] For these suspicions to be neutralised and for AI to attain legitimacy and trust in society, attendant risks must be identified, reviewed and resolved in accordance with applicable laws and taking the rights of data subjects into consideration.

The lack of adequate data protection laws in African countries will make the continent a testing ground for data processing activities that otherwise are unlawful in the home countries of multinational data controllers, with residents of the African continent being the guinea pigs for such unlawful processing activities. The same argument will apply where the existing data protection laws are poorly enforced. In practice, it is not very difficult to find data processing activities where data controllers under the guise of providing a service unlawfully process personal data in African countries in a manner that is unlawful in their home countries.[94] While such data controllers undoubtedly act in an unethical manner,[95] it behoves Africa(ns) to change the narrative by taking the enactment and enforcement of very strict data protection laws very seriously. Another disturbing incidence of this occurrence is the violation of the right to the dignity of the human person occasioned by this violation of the right to data protection. As noted by the European data protection supervisor, 'privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of ameliorating the possible erosion of privacy and dignity through large scale personal data processing'.[96] Therefore, violations of the right to data protection are also tantamount to violations of the right to the dignity of the human person, particularly because of the close relationship between personal data and who we are and can become.[97] The possible risks that may arise from the unlawful processing operations carried out by AI are heightened by the fact that such processing operations are large scales possibly covering multiple countries. The importance of proper regulations to prevent Africa

93 'Report shows consumers don't trust artificial intelligence' *Fintech news* (4 December 2019), https://www.fintechnews.org/report-shows-consumers-dont-trust-artificial-intelligence/#:~:text=A%20new%20report%20released%20by,person%20to%20help%20make%20decisions. (accessed 15 September 2020).

94 See E Salami 'Nigerian data protection law: The effectiveness of the Nigerian Data Protection Bill as a tool for fostering data protection compliance in Nigeria' (2019) 43 *Datenschutz Datensich* 579, https://ssrn.com/abstract=3614335 (accessed 21 September 2020).

95 R Densmore *Privacy program management* (2013) 19.

96 European Data Protection Supervisor 'Opinion 4/2015: Towards a new digital ethics data, dignity and technology' (2015).

97 L Floridi 'The ontological interpretation of informational privacy' (2005) 7 *Ethics and Information Technology* 185-200.

from being a testing ground for unlawful processing activities cannot be overemphasised and must be given utmost attention.

The lack of adequate data protection regulations in the use of AI can also inhibit trade between African countries and their counterparts in countries where data protection law is properly regulated. For instance, African companies using AI for targeted marketing[98] in European Union (EU) countries will have to comply with the GDPR since they are targeting persons within the EU.[99] In today's global economy, personal data processing is a fundamental aspect of trade and business, and Africa stands to benefit significantly from having a compliant level of data protection law. Where African companies are not compliant with data protection law, their foreign counterparts will be skeptical about engaging them in businesses, thereby limiting trade for African businesses. Furthermore, the lack of data protection law will hinder the growth of businesses such as data-based businesses (for instance, 'cloud storage as a service'). This is because should the continent be tagged as being a non-compliant data protection region, such data-based businesses will not grow, which will be unfortunate on a continent that is in dire need of economic development.

7 Conclusion

Based on the analysis carried out in this chapter, Africa (and African countries) must re-examine their data protection laws to ensure that data protection law complies with the realities of an AI. Based on the focus legislations, decent data protection laws are already in existence across the continent, and two major steps are needed if African countries are to consolidate on this in the use of AI. First, Africa and African countries must be willing to revisit some of the provisions in their data protection legislations to permit amendments that arise in light of AI. Second, supervisory and regulatory authorities must take the enforcement of data protection somewhat more seriously be publishing guidance documents, making regulations to plug new gaps identified in the law, investigating alleged violations of data subject rights, conducting random audits, etc. Through these measures, the continent can control the impact of AI within the context of AI and reduce the mistrust that it has gathered overtime, thereby giving AI more legitimacy as a useful addition to the human society. Failure to do this will result in the violation of the data

98 AI systems have been developed for use in targeted marketing. See 'How AI is used in targeted marketing' (17 September 2020), https://azati.ai/artificial-intelligence-targeted-marketing/ (accessed 21 September 2020).

99 See art 3 GDPR.

protection rights of a vast number of Africans and will slow down the acceptance of AI into the mainstream of the African economic life.

References

Adaramola, Z 'Why Africa is backward in technology – NOTAP' (21 June 2012, All Africa)

Bello, I 'Beginners' guide to artificial intelligence "AI"' (17 July 2017) Medium

Bode, K 'Researchers find "anonymized" data is even less anonymous than we thought' (Motherboard)

Boyd, D & Crawford, K 'Six provocations for big data' A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011

Bygrave, L A Data Protection Law: Approaching Its Rationale, Logic and Limits Information Law Series, Volume 10, (2002) 58.

Bygrave, LA 'Article 22. Automated individual decision-making, including profiling' in Kuner, C, Bygrave, LA & Docksey, C (eds) *The EU General Data Protection Regulation (GDPR): A commentary* (OUP 2020)

Carey, P *Data protection: A practical guide to UK and EU law* (OUP 2018)

Castelluccia, C & Le Métayer, D 'Understanding algorithmic decision-making: Opportunities and challenges' European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 624.261 – March 2019

Cowgill, B and others 'Biased programmers? Or biased data? A field experiment in operationalising AI ethics' in Proceedings of the 21st ACM Conference on Economics and Computation (1 June 2020) 2

Crabtree, A and others 'Privacy by design for the internet of things: Building accountability and security' (13 July 2020, SSRN)

Enev, M and others 'Automobile driver fingerprinting' (2016) 1 *Proceedings on Privacy Enhancing Technologies*

Faggella, D 'Artificial intelligence applications for lending and loan management' (3 April 2020, Emerj)

Ferguson, AG *The rise of big data policing: Surveillance, race, and the future of law enforcement* (New York University Press2017)

Finlay, S *Artificial intelligence and machine learning for business: A no-nonsense guide to data driven technologies* (2018)

Floridi, L & Taddeo, M 'What is data ethics?' Oxford Internet Institute (2016) 5

Floridi, L 'The ontological interpretation of informational privacy' (2005) 7 *Ethics and Information Technology* 185

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

Hao, K 'AI is sending people to jail and getting it wrong' (2019 *MIT Technology Review*

Harmon, A 'As cameras track Detroit's residents, a debate ensues over racial bias' *The New York Times* (18 July 2019) recognition-

Harrington, C 'Improving access to sexual health education in Kenya with artificial intelligence' (15 January 2020, Humans of Machine Learning)

Herrmann, A and others *Autonomous driving: How the driverless revolution will change the world* (Emerald Publishing 2018)

Hillman, NL 'The use of artificial intelligence in gauging the risk of recidivism' (1 January 2019, ABA)

Jackson, H 'Information provision obligations' in Ustaran, E (ed) *European data protection law and practice* (International Association of Privacy Professionals 2018)

Kaplan, J *Artificial intelligence: What everyone needs to know* (OUP 2016)

Koroma, DSM 'Traditional forms of communication of the Malimba of Sierra Leone' (2018) 10.

Lachlan, U & Jiahong, C 'On the principle of accountability: Challenges for smart homes and cybersecurity' (17 June 2020)

Malik, N & Singh, PV 'Deep learning in computer vision: Methods, interpretation, causation and fairness' (28 May 2019)

Malinga, S 'SA not ready for autonomous vehicles' (7 October 2020, ITWeb)

McCarthy, J 'What is artificial intelligence?' (12 November 2007), http://jmc.stanford.edu/articles/whatisai.html (accessed 10 September 2020)

Melendez, C 'Data is the lifeblood of AI, but how do you collect it?' (8 August 2018, Infoworld)

Miriri, D 'Rwandan medical workers deploy robots to minimise coronavirus risk' (5 June 2020, World Economic Forum)

O'Keefe, K & O'Brien, D *Ethical data and information management* (Kogan Page 2018)

Odutola, A 'FG acquires profiling robots for airport' (27 June 2020, Nairametrics)

Pierce, R 'Machine learning for diagnosis and treatment: Gymnastics for the GDPR' (2018) 4 *EDPL* 339

Rosen, JW 'Zipline's ambitious medical drone delivery in Africa' (8 June 2017, MIT Tech Review)

Russell, SJ & Norvig, P *Artificial intelligence: A modern approach* (Prentice Hall 2010)

Salami, E 'Autonomous transport vehicles versus the principles of data protection law: Is compatibility really an impossibility?' (2020) *International Data Privacy Law Journal*

Salami, E 'Nigerian data protection law: The effectiveness of the Nigerian Data Protection Bill as a tool for fostering data protection compliance in Nigeria' (2019) 43 *Datenschutz Datensich* 579

Shacklett, M 'Repurpose big data to get more analytics bang for your bucks' (28 January 2014, Tech Republic)

Shaw, TJ *DPO handbook: Data protection officers under the GDPR* (IAPP 2018)

Sorkin, DE 'Technical and legal approaches to unsolicited electronic mail' (2001) 35 USF Law Review 325

Stone, P and others 'Artificial intelligence and life In 2030: Report of the 2015-2016 Study Panel' (September 2016, Stanford.edu)

Sweeney, L 'Matching known patients to health records in Washington State data' (5 June 2013)

Tay, J and others 'Application of computer vision in the construction industry' (19 November 2019)

Turing, AM 'Computing machinery and intelligence' (1950) 59 *Mind* 433

Van der Velde, N 'Speech recognition technology overview' (8 July 2019, Globalme Language and Technology)

Voigt, P & Von dem Bussche, A *The EU General Data Protection Regulation (GDPR): A practical guide* (Springer 2017)

Wachter, S and others 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (28 December 2016) 1