The Impact of Artificial Intelligence on Data Protection and Privacy:

A Walk-through Rights of a Data Subject in Africa

May **2024**

CIPESA

Introduction

Artificial intelligence (AI), which refers to computer systems capable of performing complex tasks that historically only a human could do, such as reasoning, making decisions, or solving problems,[1] has the potential to impact various aspects of society. Today, AI is playing a critical role in digitalisation in Africa, including in countries that are developing so-called "smart cities".[2] However, there are no specific laws on AI in Africa. Efforts that exist, such as in Egypt, Ghana, Kenya, Mauritius and Rwanda, are merely policies or strategic plans.[3] Nevertheless, data protection legislation provisions such as those that bar automated decision-making relate to the use of AI. It is therefore important to explore the impact of AI on data protection and privacy and how African governments could prepare to deal with AI to check data and privacy breaches.

1 *What Is Artificial Intelligence? Definition, Uses, and Types, https://www.coursera.org/articles/what-is-artificial-intelligence*

2 *Victor Oluwole, Africa's smartest cities: Top countries embracing urbanisation and technology," Business Insider Africa, July 28, 2023, https://africa.businessinsider.com/local/lifestyle/africas-smartest-cities-top-countries-embracing-urbanisation-and-technology/hszfjqk*

3 *Rachel Adam, AI in Africa: Key Concerns and Policy Considerations for the Future of the Continent, APRI May 30, 2023, https://afripoli.org/ai-in-africa-key-concerns-and-policy-considerations-for-the-future-of-the-continent*

The Rights and Principles of Data Protection

36 African countries

have enacted data protection and privacy laws

At least 36 African countries have enacted data protection and privacy laws that regulate the collection and processing of personal data.[4] Similarly, the African Union Convention on Cyber Security and Personal Data Protection which was adopted in 2014 to establish a legal framework for cybersecurity and personal data protection entered into force in June 2023.[5]

Moreover, several countries have enacted laws covering computer misuse, cybersecurity, electronic signatures, and electronic commerce. These laws also protect individuals from abuse and violation of rights when technologies are used in data collection, control and processing.

Rights of Data Subjects

Across different countries, data protection rights mirror those laid down in regional and international human rights instruments such as the African Union Convention on Cyber Security and Personal Data Protection,[6] the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[7] and the General Data Protection Regulation (GDPR) of Europe.[8] These rights include the right to access personal information, the right to prevent the processing of personal data, and the right of individuals to be informed of the intended use of their personal data, including in cases of automated data processing where the decision significantly affects the data subject.

Furthermore, the data subject has a right to access personal data in the custody of data collectors, controllers and processors, the right to object to the processing of all or part of their personal data, the right to rectification, blocking, erasure and destruction of personal data, and the right to a remedy in case of data privacy breaches.

The rights of the data subject often go hand-in-hand with data protection principles which are elaborated in national laws. Below are the common principles:

4 *See for instance, Data Protection Africa, https://dataprotection.africa/*

5 *See "Status List" at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf*

6 *African Union Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf*

7 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://one.oecd.org/document/C(2013)79/en/pdf*

8 *General Data Protection Regulation (GDPR), https://gdpr-info.eu/*

Data Protection Principles

Lawfulness, fairness and transparency: Processing of personal data should be done lawfully and fairly, and data subjects should be consulted to ensure transparency.

Purpose limitation or specification: Personal data must be collected for a specific purpose and a lawful purpose.

Storage Limitation: The data must be retained for a period which the purpose serves.

Data minimisation: Personal data should be processed for a specified purpose and should be relevant, adequate and not excessive.

Accuracy: All personal data that is collected should be complete, accurate, up-to-date and not misleading.

Integrity and confidentiality (security): Security safeguards should be in place for personal data to ensure the integrity and confidentiality of data and to safeguard the data against loss or damage and unlawful access.

Accountability: The responsible party should ensure that all measures and conditions in place are complied with to ensure that all principles are given effect.

The rights of the data subject ensure that the individual has control over how their data is collected, managed and processed. Thus, these rights create the basis for data collectors, controllers and processors to be accountable and transparent when dealing with personal data. However, with the advancement of AI, there are concerns as to whether automated systems whose tasks are often programmed can respect data protection rights or adhere to accountability and transparency when dealing with personal data.

What has AI got to do with Data Rights?

The advent of AI raises challenges for data protection in sectors such as transportation, banking, health care, retail, and e-commerce, where mass data is collected. Mass collection of data is further enhanced by the use of AI chatbots and voice assistants (use of language and generation of responses); crowdsourcing, where data is collected from organisations, individuals and intermediaries; web scraping and crawling (the collection of data from public or online platforms), and by associated systems such as Google Maps, marketing sites and social media and networking platforms. Mass data stored in large databases faces potential threats and risks since it is often prone to attacks, illegal access or sharing with third parties.

A key challenge posed by AI to data is the potential for violation of privacy[9] especially through data breaches and unauthorised access to personal information.[10] Additionally, AI raises issues of bias and discrimination when dealing with data, perpetrating abusive data practices, spreading misinformation and disinformation, enhancing and enabling real-time surveillance, and aggravating cyber-attacks such as phishing through the manning of malicious links. Below, we explore ways through which AI affects data rights.

Right to Access Personal Information

The right to access requires that data subjects are provided with information, including the justification for collecting data, identification of the data controller, and categories of data to be collected. Most access-related rights require skilled and competent staff to ensure that the necessary steps and precautions are taken to observe and guarantee the right to access personal information.

AI systems are usually programmed to handle specific kinds of data. Their capacities are limited to the built-in competencies of the tasks they can man. This means that they are rather inflexible and may not observe the rights of data subjects. In the long run, while AI could manage and ease the process of access to information, some categories of personal information may be left out from access by data subjects. Artificial intelligence can be used to violate privacy and perpetuate data privacy breaches since AI programmes may be inclined to particular kinds of data, including through discrimination in making decisions to otherwise would be similar questions and needs of data subjects.[11]

9 *Cujo LLC, Why Artificial Intelligence Design Must Prioritize Data Privacy, https://www.weforum.org/agenda/2022/03/designing-artificial-intelligence-for-privacy/?ref=thedigitalspeaker.com*

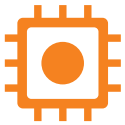
10 *The Economic Times, AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data, https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms*

11 *European Union Agency for Fundamental Rights, Bias in algorithms - Artificial Intelligence and Discrimination 2022, https://fra.europa.eu/sites/default/files/fra_uploads/-fra-2022-bias-in-algorithms_en.pdf*

Right to Object to Processing of Personal Data

The right to object to the processing of personal data is important for verifying the accuracy of data in the interest of the data subject. The use of AI is likely to fall short of accuracy, lawfulness, and purpose of data since it cannot determine and separate accurate from inaccurate data, the extraction of data based on purpose, or the specification or processing of for lawful purposes data as distinguished from unlawful processing.[12]

Artificial intelligence thus presents challenges to data principles and rights in dealing with the right to objection to data processing. Furthermore, amidst the use of AI, there is no assurance that technology has been prepared to comply with rights and principles. It therefore leaves privacy and use of data at stake of potential abuse and rights violation since AI operates based on programming with, at times no capacity to distinguish prohibited from accepted data practices.



Rights in Relation to Automated Decision-Making

The essence of this right is that automated decisions are not made against the data subject solely based on technologies with no human involvement. The effects of automated decision-making such as profiling extend to unlawful data breaches that could potentially or adversely affect the data subject.

With AI, interpretation of data can be inaccurate or lead to unfair conclusions. Such automated decision-making, based on personal data such as ethnicity, race, gender, religion and political inclination may lead to discriminatory practices, which in turn undermines proper decision-making and accountability.[13]

According to the Rodrigues Journal of Responsible Technology, automated decision-making has wide impacts on human rights and freedoms of the data subject, such as privacy, freedom of movement, expression and access to information and autonomy to participate or not to participate, since in some instances AI often operates without human intervention.[14] The non-involvement of a human figure and sole basis on algorithms in decision-making not only deprives individuals of their rights and freedoms but also the ability to question decisions that fundamentally affect them.[15]

12 *OVIC, Artificial Intelligence and Privacy Issues and Challenges, https://ovic.vic.gov.au/wp-content/uploads/2021/04/Artificial-Intelligence-and-Privacy-Issues-And-Challenges.docx*

13 *Bietti, Elettra. Data is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR.*

14 *Rodrigues, Rowena. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities, https://tadbirsaz.org/assets/filemanager/userfiles/research/%D8%AD%D9%82%D9%88%D9%82/Legal-and-human-rights-issues-of-AI.pdf*

15 *Walsh, Toby. It's Aive!: Artificial Intelligence from the Logic Piano to Killer Robots. La Trobe University Press, 2017, pp 150-151.*

Rectification and Erasure

To ensure the accuracy of collected and processed data, the data subject has a right to rectification and erasure of data. The right to rectification relates to dealing with inaccurate, outdated, misleading, incomplete or erroneous data. Erasure deals with circumstances that permit the data subject to request the data controller to stop any further processing or to erase personal data, especially when there is no legal basis for the retention of such data. The justification lies in the need to ensure decisions do not adversely affect data subjects because of incorrectness or inaccuracy.

Accurate and complete data facilitates proper and effective planning for the populace which could lead to improved service delivery in areas such as health, education, water and other infrastructural development. It can also lead to the assurance that services go to the intended persons.

Rectification and erasure require human intervention if the accuracy of data is to be guaranteed. Human intervention aids the proper establishment and diagnosis of existing problematic data issues to perform rightful rectification and erasure. AI systems that do not comprehend privacy issues may not be as transparent as human interventions and thus may not help individuals fully understand the use and control of their data.[16]

Also, such AI systems may fail to ensure that requests from data subjects to delete or erase data are handled promptly. In other instances, AI may never take the actions placed by data subjects regarding their data. Moreover, due to the complexity of systems, some AI systems may not accurately comply with the erasure requirement. In other cases, some AI may deal with the erasure requirement based on bias against data subjects. Worse still, they may erroneously identify and erase critical data and restore with wrong data sets if not regulated or run ethically.[17]

Indeed, most laws require data controllers to take reasonable steps, including technical measures to respond to requests by data subjects to delete personal data perceived to be unlawful, inaccurate, misleading, or malicious.[18] This is a straightforward case that requires direct human intervention beyond AI.

16 *Villaronga, Eduard Fosch, Peter Kieseberg, and Tiffany Li. Humans Forget, Machines Remember: Artificial Intelligence and the Right to be Forgotten, https://scholarship.law.bu.edu/c-gi/viewcontent.cgi?article=1816&context=faculty_scholarship*

17 *FRA, EU. Data quality and artificial intelligence–mitigating bias and error to protect fundamental rights. (2017), https://fra.europa.eu/sites/default/files/fra_uploads/-fra-2019-data-quality-and-ai_en.pdf*

18 *Ibid.*

Right to Data Portability

In some data protection laws in Africa, the right to data portability is not pronounced as a data subject's entitlement. The right to data portability involves receiving personal data in a simple and machine-readable format from the data controller[19] and the ability to easily transmit the data to another data controller where required.[20] Data portability, which provides opportunities for data transfer from one company to another or across government agencies to inform development and economies, promotes healthy competition in sectors and eases data exchange. However, AI presents privacy challenges to portability, which often could aggravate the confidentiality risk. Some AI systems can perpetuate data lock-in as systems may be designed to make it impossible for data to be ported or for individuals to switch to other services.

Artificial intelligence can facilitate indiscriminate movement of data, including data which is irrelevant to the purpose for which the data is needed.[21] For instance, if the movement of data is for purposes of the banking sector and its clientele base, data moved by AI may not necessarily be required when data on the frequency of transactions is moved due to lack of human intervention. Artificial intelligence systems may also promote discrimination as to who can or should access certain sets of data, services or products based on stored data.

Similarly, AI may lead to exposure of individuals' habits such as sites that are frequently accessed and consumed. While it can help reduce switching costs, unauthorised access to ICT tools belonging to a particular individual may expose their private information since AI may not ably distinguish users of digital services.[22]

Moreover, the use of AI in data portability may become misleading for individuals when wrong data is shared to inform habits and traffic in business, and in access and use of goods and services. In other cases, wrong data may arise from the use of the various encryption practices by data controllers which may result in the communication of wrong data. In such cases, data portability may lead to the use of wrong data and data beyond purpose.[23] As such, data controllers and processors can mislead one to embrace and use poor-quality goods and services with reliance on information moved between a highly reputable entity with one that is not comparable.

19 *Zufall, Frederike, and Raphael Zingg. Data Portability in a Data-Driven World. In Data Regulation as Artificial Intelligence Regulation, pp. 215-234. 2021.*

20 *See the European Union General Data Protection Regulation, article 20, https://gdpr-info.eu/art-20-gdpr/*

21 *Data portability and Interoperability: A Primer on Two Policy Tools for Regulation of Digitized Industries, https://www.brookings.edu/research/data-portability-and-interoperability-a-primer-on-two-policy-tools-for-regulation-of-digitized-industries/*

22 *Ibid.*

23 *Ibid.*

Right to Effective Remedy

Data subjects have a right to an effective remedy against data controllers and processors when their rights are violated. Data rights are violated during data processing and in cases of non-compliance with the law. The right to remedy extends to appeals where the data subject is not content with the decision concerning data breaches.

The role of AI in accessing an effective remedy is straightforward. What is not in doubt is that AI has the potential to violate and perpetrate abuse of the rights of the data subject. However, there is no clearly established mechanism where AI analyses cases of justice and issues an appropriate remedy. The level of involvement of AI relates more to violation while the entertainment and determination of violation requires human intervention. Human intervention often ensures that human rights or the rule of law meet the requisite standards in dispute resolution or complaints handling mechanisms.

Human intervention at this level does not seek to undermine the fact that with the emerging developments, advancement and evolution in technology, AI will entertain and decisively determine cases of data breaches and issue appropriate remedies. It is possible. But artificial intelligence still remains largely opaque in how rules of remedy should be applied. AI may not ably comprehend various languages and the uniqueness of procedures which it is often not adapted to suit different contexts or conceptions of justice.

Conclusion

The evolution of AI presents opportunities and challenges for personal data. With increased digitalisations, data subjects may have no option but to surrender data to AI systems in order to access goods and services including from government and financial institutions, and in business and trade. Amidst the challenges and ethical considerations posed, maintaining a balance between innovation and privacy protection is crucial. This balance can be achieved through reinforcing legal and regulatory frameworks, advocating for transparency and accountability, and cultivating education and awareness. Through this approach, it is possible to leverage the advantages of AI while ensuring the protection of the fundamental rights and privacy of individuals.

Recommendations

The following are the emerging recommendations for the key stakeholders' consideration if AI is to be effectively applied in personal data processing in Africa.

Governments and Decision Makers

- Work towards establishing all mechanisms that provide all information on AI to data subjects to enhance their capacity to participate and make informed decisions in the processes that involve processing of their personal data.
- Ensure that the use of AI adheres to and complies with the accountability requirements at all stages. Embedding accountability in AI processes allows risk assessments and evaluation to minimise potential data privacy risks.
- Invest widely in technology development, including research and innovation for privacy sensitive AI.
- Develop policies and laws that seek to openly and transparently regulate AI, including its development and usage.

Developers and Service Providers

- Developers and Users of AI should ensure that AI systems are sufficiently and efficiently trained and equipped to handle big data.
- Developers should ensure that the rights of data subjects are protected especially during the collection and processing of personal data.
- Data processors who wish to rely on AI should conduct data privacy impact assessments to establish the potential impacts of AI technologies on privacy and develop effective checks on possible data breaches.
- Artificial intelligence systems should be constantly audited to ensure that they comply with data protection standards and specifically prevent any cases of bias that would lead to unfair data practices.
- Automated decision-making should be conducted under very strict limitations. Where necessary, human intervention by competent authorities and persons should be made possible so as to weed out any cases of injustice.

Civil Society Organisations and Academia

- Continually advocate for the ethical use of AI in the management of personal data by data processors.
- Conduct evidence-based research on the use of AI and its associated effects on personal data and data security, as well as on personal data ethics.
- Build the capacity of individuals and institutions to fully understand and respond to AI issues including taking relevant precautionary measures against potential risks posed by AI.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
+256 414 289 502
programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org