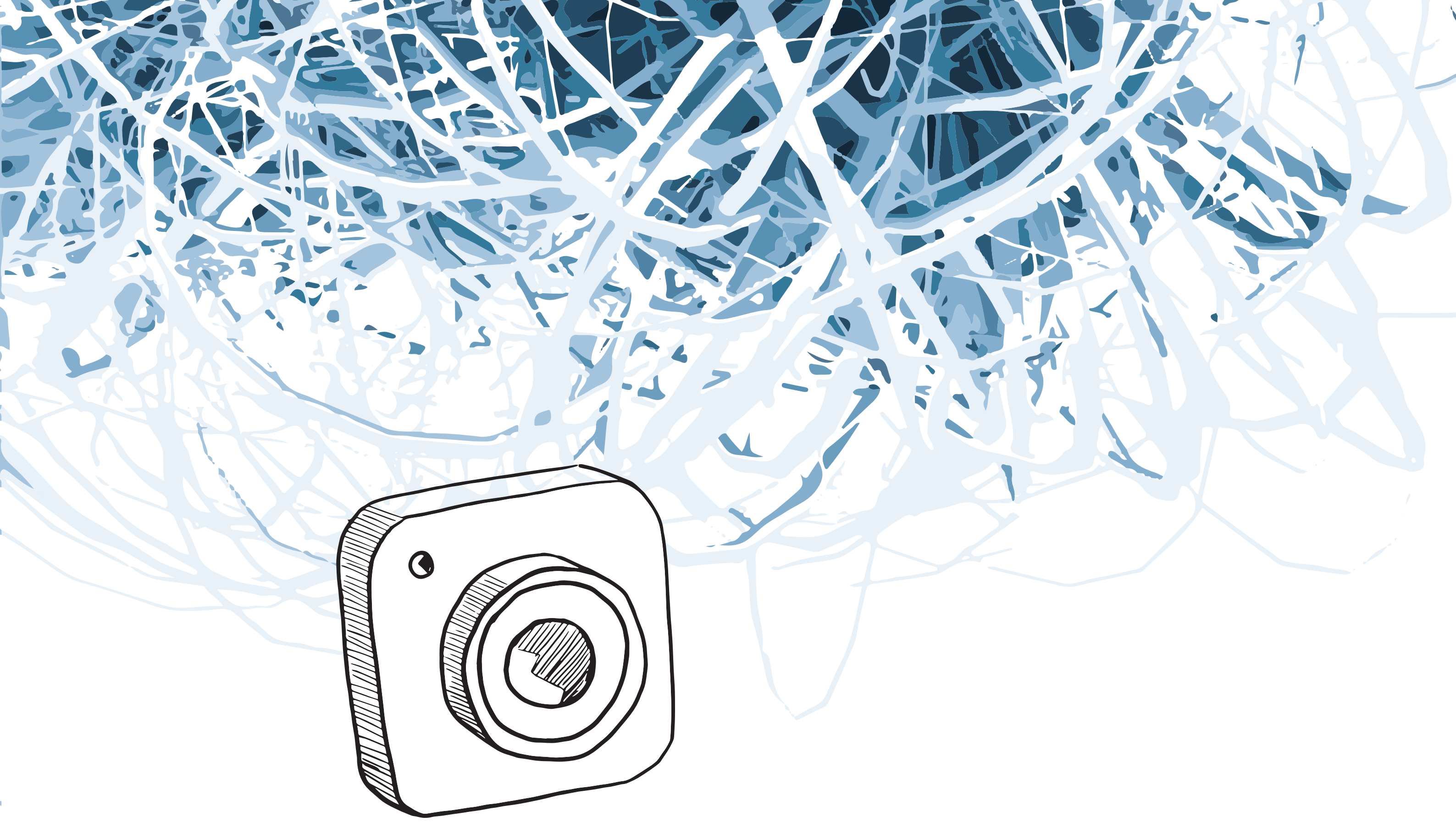
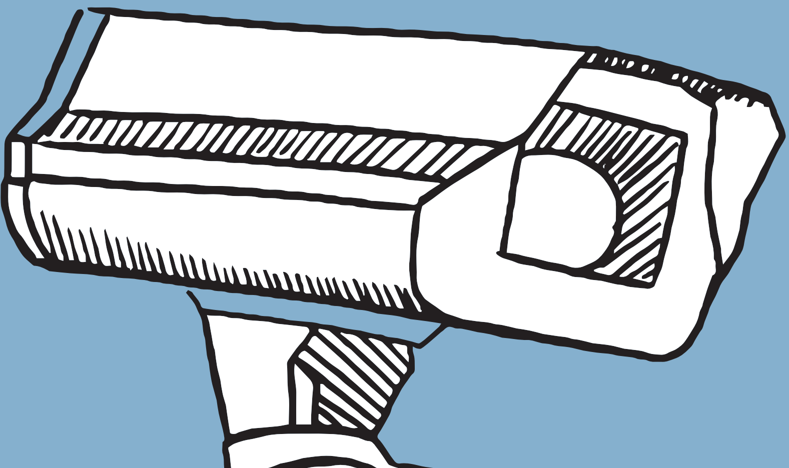


UNVEILING PRIVACY IN THE AI ERA: NAVIGATING SURVEILLANCE, ETHICS, AND EQUITABLE SOLUTIONS

A research project charting the course of privacy in AI surveillance

Strathmore University

Centre for Intellectual Property and Information Technology Law



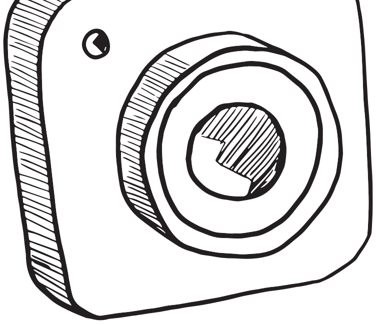


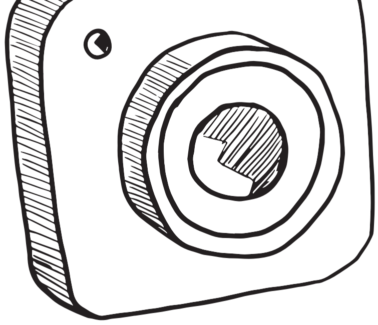
TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The completion of this comprehensive report on privacy in AI surveillance has been a collaborative effort, shaped by the contributions and support of numerous individuals and organisations. We extend our heartfelt gratitude to those who have played a vital role in making this endeavour possible.

We would like to express our sincere appreciation to the experts, scholars, and professionals who provided valuable guidance and input throughout the research process. Your contributions have contributed significantly to shedding light on the critical issues at hand and charting a path toward a more inclusive and digitally equitable future for all. This report is a collaborative effort based on the inputs of the CIPIT Artificial Intelligence Centre Team that includes; Research Fellow Valerie Kutima and Research Assistant Doreen Aoko Abiero. Gloria Muthoka was also instrumental in coming up with the design for the infographic related to this report.

Our acknowledgment also extends to the global initiatives and best practices that have informed our recommendations. The lessons learned from various jurisdictions have provided invaluable insights into effective strategies for addressing privacy in AI surveillance.



1.0 Introduction

In the rapidly evolving digital landscape, the integration of artificial intelligence (AI) in surveillance technologies has presented unprecedented opportunities and challenges for privacy. This report investigates the intricate relationship between surveillance, AI, and privacy, elucidating the importance of privacy in the digital era, the multifaceted risks posed by AI-driven data processing, the role of biases and discrimination, the implications of job displacements, data abuse practices, the dominance of Big Tech, data collection and use by AI, and the global approaches and best practices to protect privacy in this context. Through an interdisciplinary lens, this report aims to provide a comprehensive understanding of the complexities and ethical considerations surrounding surveillance and privacy in the age of AI.

Surveillance involves observing, recording and categorising information about people, processes and institutions[1]. It has also been defined as the collection and analysis of information about populations in order to govern their activities.[2] Privacy, on the other hand, has been defined as the right to be let alone, or freedom from interference or intrusion[3]. Information privacy has been defined as the right to have some control over how your personal information is collected and used.[4]

In the contemporary digital landscape, the significance of privacy cannot be overstated, given the profound influence of technology and the internet on our daily lives. Privacy safeguards individuals from potential threats such as identity theft, cyberstalking, harassment, and other forms of digital crimes. Without adequate privacy measures, people's personal information and sensitive data become vulnerable to malicious actors who can misuse it for nefarious purposes.[5]

In the digital age, vast amounts of data are generated and collected by various organisations, including governments and corporations.[6] Protecting individuals' privacy

[1] Christian Fuchs, "How can Surveillance be Defined? Remarks on Theoretical Foundations of Surveillance Studies" (1 October 2010) <http://sns3.uti.at/wp-content/uploads/2010/10/The-Internet-Surveillance-Research-Paper-Series-1-Christian-Fuchs-How-Surveillance-Can-Be-Defined.pdf > accessed 7 August 2023.

[2] ibid

[3] iapp, "What does privacy mean?" <https://iapp.org/about/what-is-privacy/ > accessed 7 August 2023.

[4] ibid

[5] Prevention and mitigation measures against phishing emails: a sequential schema model, Yumi E Suzuki, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8478002/ accessed on 24 August 2023.

[6] Digital technologies: tensions in privacy and data, Sara Quach, https://link.springer.com/article/10.1007/s11747-022-00845-y accessed on 24 August 2023.

> Trust is the foundation of any successful digital service or online interaction. Users are more likely to engage with technology and share their information when they believe their privacy is protected.

ensures that this data is handled responsibly and ethically, preventing unauthorised access or data breaches that could lead to devastating consequences for individuals and society. Privacy allows individuals to exercise control over their personal information and make autonomous decisions without the fear of judgment, discrimination, or manipulation.[7] It fosters a sense of independence and empowers individuals to express themselves freely without the fear of constant surveillance.

Trust is the foundation of any successful digital service or online interaction. Users are more likely to engage with technology and share their information when they believe their privacy is protected. By respecting privacy, businesses and institutions can build trust with their users and customers, enhancing long-term relationships.

In a digital society, the free flow of information and ideas is vital for the functioning of democracy.[8] Privacy protects individuals engaged in political discourse or activism from surveillance, censorship, or reprisals, ensuring that diverse voices can participate freely.[9] Without proper privacy protections, individuals may be subjected to discriminatory practices based on their personal information, such as race, religion, gender, or other characteristics.[10] Privacy regulations help mitigate such risks and promote fairness and equality. Striking a balance between privacy and data access can lead to ethical data-driven innovation.[11] Respecting privacy while leveraging data for research and development can yield significant societal benefits without compromising individuals' rights. This report will delve into several critical aspects of the AI landscape, encompassing data collection and utilisation by AI technologies, the integration of AI in surveillance, emerging AI-related privacy concerns, the formidable challenges in upholding privacy during the AI revolution, international strategies for safeguarding privacy in the era of AI, and the adoption of best practices and mitigation measures for preserving privacy and ensuring data protection in AI applications.

1.1 Data Collection and Use by AI Technologies

AI heavily relies on data collection for training and performance improvement. This involves data collection from various sources like user interactions, sensors, text, and images. After collecting data, it's processed and organised.

[7] ibid.

[8] ECHR, Guide on Article 10, https://www.echr.coe.int/documents/d/echr/guide_art_10_eng accessed on 24 August 2023.

[9] Media and Good Governance Report, UNESCO, https://unesdoc.unesco.org/ark:/48223/pf0000146311 accessed on 24 August 2023.

[10] Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?, Marvin Van Bekkum, https://www.sciencedirect.com/science/article/pii/S0267364922001133 accessed on 24 August 2023.

[11] Privacy, Ethics, and Data Access: A Case Study of the Fragile Families Challenge, Ian Lundberg, https://journals.sagepub.com/doi/10.1177/2378023118813023 accessed on 24 August 2023.

In supervised learning, human annotators label the data.[12] AI models are then trained using this data, adjusting their parameters to improve performance. Learning doesn't stop here; AI models can adapt over time through ongoing interactions.

Once trained, AI models are deployed for real-world applications in a process called inference.[13] They process new data to make predictions or provide recommendations. AI often personalised user experiences based on collected data, like tailored content or product suggestions. However, extensive data use by AI raises privacy concerns about data security and misuse. Addressing these concerns is vital for maintaining user trust and ensuring ethical AI development.

Kenya, recognizing the significance of data protection in the digital age, enacted the Data Protection Act in 2019.[14] This legislation establishes a robust framework for safeguarding personal data, providing individuals with control over their information. Under this act, individuals have the right to access their data held by data controllers and demand its correction or deletion. Section 25 of the Act outlines the provisions concerning automated decision-making, which is relevant in the context of AI surveillance systems that make decisions based on algorithms.[15] Moreover, the Kenyan Constitution in Article 31 enshrines the right to privacy.[16] This constitutional provision resonates with the global recognition of privacy as a fundamental human right, emphasising the need to protect personal data from unauthorised access and usage.

1.2 The Use of AI in Surveillance

The rise of AI in surveillance brings forth a multitude of possibilities and challenges, driven by technologies like computer vision, facial recognition, and behavioural analysis.[17] These technologies aim to enhance monitoring and analysis capabilities across various sectors, from public spaces to traffic networks and airports, offering more efficient and comprehensive supervision.[18]

AI algorithms excel in object recognition, accurately identifying and tracking objects, faces, and vehicles in real-time video feeds.[19] Facial recognition, a prominent application, raises concerns about privacy infringement and civil liberties, despite its potential for identification and tracking.[20]

Predictive analytics integrated into surveillance systems can detect security threats and anomalous behaviour, allowing for preemptive security measures.[21] In the realm of public safety and crime prevention, AI-powered surveillance aids law enforcement agencies in tracking criminals and enhancing safety measures.[22]

[12] AI Multiple, "AI Data Collection in 2023: Guide, Challenges & 4 Methods," https://research.aimultiple.com/data-collection/ accessed on 12 September 2023.

[13] Label Your Data, "What Is Data Collection in Machine Learning?" https://labelyourdata.com/articles/data-collection-methods-AI accessed on 12 September 2023.

[14] Data Protection Act, 2019 (Act No.24 of 2019).

[15] ibid.

[16] Constitution of Kenya, 2010.

[17] Shaik Mohammed Zahid, T. Nashiya Najesh, Salman. K, Shaik Ruhul Ameen and Anooja Ali. "A Multi Stage Approach for Object and Face Detection using CNN." 2023 8th International Conference on Communication and Electronics Systems (ICCES) (2023): 798-803. https://doi.org/10.1109/ICCES57224.2023.10192823. accessed 26 August 2024.

[18] A. Mhalla, T. Chateau, S. Gazzah and N. Amara. "An Embedded Computer-Vision System for Multi-Object Detection in Traffic Surveillance." IEEE Transactions on Intelligent Transportation Systems, 20 (2019): 4006-4018. https://doi.org/10.1109/TITS.2018.2876614. accessed 26 August 2024.

[19] D. N. L. Prasanna, Ch Janaki Annapurna, G. Yeshwanth, G. S. Shabina and Prema Tejalingam. "Real-Time Object Detection." international journal of food and nutritional sciences (2023). https://doi.org/10.48047/ijfans/v11/i12/207. accessed 26 August 2024.

[20] Latika Kharb and Deepak Chahal. "Privacy Threats in Facial Recognition-Based Identity Verification." International Journal of Advanced Research in Science, Communication and Technology (2023). https://doi.org/10.48175/ijarsct-11686. accessed 26 August 2024.

[21] Huu-Thanh Duong, Viet-Tuan Le and Vinh Truong Hoang. "Deep Learning-Based Anomaly Detection in Video Surveillance: A Survey." Sensors (Basel, Switzerland), 23 (2023). https://doi.org/10.3390/s23115024. accessed 26 August 2024.

[22] Paria Sarzaeim, Q. Mahmoud, Akramul Azim, Gary Bauer and Ian Bowles. "A Systematic Review of Using Machine Learning and Natural Language Processing in Smart Policing." Computers (2023). https://doi.org/10.3390/computers12120255. accessed 26 August 2024.

Traffic management benefits from AI's real-time analysis of traffic data, optimising traffic flow and road safety by identifying congestion and adjusting traffic signals accordingly.[23] Remote monitoring enables access to surveillance from a distance and instant alerts for suspicious activities.[24]

However, the proliferation of AI surveillance poses significant privacy and ethical dilemmas. Mass surveillance risks violating individuals' privacy rights, leading to extensive monitoring of innocent citizens.[25] Biases and misidentifications in facial recognition systems disproportionately affect minority groups, resulting in wrongful arrests and discrimination.[26]

Transparency and accountability issues arise as AI surveillance systems often operate opaquely, leaving those under surveillance unaware of data collection, usage, and storage details.[27] The absence of comprehensive legal and regulatory frameworks has created uncertainty about proper implementation and the potential for misuse.[28]

The broader consequences of mass surveillance include potential chilling effects on society, hindering free speech and expression due to widespread observation.[29] Balancing the advantages of AI-powered surveillance with these ethical and privacy concerns remains a complex challenge.

1.4 Challenges in Preserving Privacy Amidst the AI Revolution: Risks and Issues in AI-driven Data Processing

The age of AI brings with it numerous benefits and opportunities, but it also introduces several privacy challenges and risks associated with AI-driven data processing.[30] AI systems rely heavily on vast amounts of data to train and improve their performance.[31] However, this creates privacy concerns as sensitive and personal data could be used without proper consent or security measures, leading to potential data breaches or unauthorised access.[32]

AI algorithms may unintentionally perpetuate biases present in the training data.[33] When these algorithms are used for decision-making processes like hiring or lending, it can lead to unfair outcomes and discrimination, raising ethical and privacy concerns.[34] AI technologies

[23] Rishabh Jain, Sunita Dhingra, Kamaldeep Joshi, A. Rana and Nitin Goyal. "Enhance traffic flow prediction with Real-Time Vehicle Data Integration." Journal of Autonomous Intelligence (2023). https://doi.org/10.32629/jai.v6i2.574. accessed 26 August 2024.

[24] D. Raja, Sheelambigai P, Sruthi Meera P and Valarmathi K. "Suspicious Activity Monitoring System using Machine Learning." 2023 8th International Conference on Communication and Electronics Systems (ICCES) (2023): 1-5. https://doi.org/10.1109/ICCES57224.2023.10192786. accessed 26 August 2024.

[25] Debasish Nandy. "Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns." Journal of Current Social and Political Issues (2023). https://doi.org/10.15575/jcspi.v1i1.442. accessed 26 August 2024.

[26] C. Tredoux, Ahmed M. Megreya, Alicia Nortje and Kate Kempen. "Changes in the own group bias across immediate and delayed recognition tasks." South African Journal of Science (2023). https://doi.org/10.17159/sajs.2023/12126. accessed 26 August 2024.

[27] B. R. Ardabili, Armin Danesh Pazho, Ghazal Alinezhad Noghre, Christopher Neff, Sai Datta Bhaskararayuni, Arun K. Ravindran, Shannon Reid and Hamed Tabkhi. "Understanding Policy and Technical Aspects of AI-enabled Smart Video Surveillance to Address Public Safety." Computational Urban Science, 3 (2023). https://doi.org/10.1007/s43762-023-00097-8. accessed 26 August 2024.

[28] Laura Lucaj, Patrick van der Smagt and Djalel Benbouzid. "AI Regulation Is (not) All You Need." Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (2023). https://doi.org/10.1145/3593013.3594079. accessed 26 August 2024.

[29] Daragh Murray, P. Fussey, Kuda Hove, W. Wakabi, Paul Kimumwe, Otto Saki and A. Stevens. "The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe." Journal of Human Rights Practice (2023). https://doi.org/10.1093/jhuman/huad020. accessed 26 August 2024.

[30] Sakib Shahriar, Sonal Allana, Seyed Mehdi Hazratifard and Rozita Dara. "A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle." IEEE Access, 11 (2023): 61829-61854. https://doi.org/10.1109/ACCESS.2023.3287195. accessed 26 August 2024.

[31] Omar Y. Al-Jarrah, Paul Yoo, S. Muhaidat, G. Karagiannidis and K. Taha. "Efficient Machine Learning for Big Data: A Review." Big Data Res., 2 (2015): 87-93. https://doi.org/10.1016/j.bdr.2015.04.001. accessed 26 August 2024.

[32] Privacy and artificial intelligence: challenges for protecting health information in a new era, Blake Murdoch, https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-021-00687-3 12 September 2024.

[33] Lakshitha R Jain and Vineetha Menon. "AI Algorithmic Bias: Understanding its Causes, Ethical and Social Implications." 2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI) (2023): 460-467. https://doi.org/10.1109/ICTAI59109.2023.00073. accessed 26 August 2024.

[34] ibid.

The age of AI brings with it numerous benefits and opportunities, but it also introduces several privacy challenges and risks associated with AI-driven data processing.

can potentially re-identify individuals from supposedly anonymized data sets by cross-referencing them with other available information. This undermines the promise of anonymity and poses risks to individuals' privacy.[35]

AI-powered surveillance technologies, such as facial recognition systems and behavioural analysis tools, can significantly erode privacy by constantly monitoring and tracking individuals without their knowledge or consent.[36] AI-driven applications often collect large amounts of data, sometimes beyond what is necessary for the intended purpose.[37] This practice raises concerns about data minimization and puts individuals' privacy at risk.[38] The use of AI may involve the transfer of data across international borders.[39] Divergent privacy regulations in different countries can create challenges in ensuring consistent privacy protection for users.[40] AI systems, particularly in the realm of online advertising and social media, may share user data with third parties for profiling and targeted advertising.[41] This can lead to privacy violations and manipulation of users' behaviour.[42] AI models can be vulnerable to adversarial attacks, where malicious actors intentionally manipulate data inputs to deceive the AI system or compromise its integrity.[43] Such attacks can lead to privacy breaches and misinformation. Obtaining informed consent from users can be challenging, especially when users are unaware of how their data is being used or lack a clear understanding of AI and its implications on their

[35] Predictive privacy: Collective data protection in the context of artificial intelligence and big data, Rainer Mühlhoff, https://journals.sagepub.com/doi/10.1177/20539517231166886 accessed 12 September 2024.

[36] The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks, Denise Almeida, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8320316/ accessed 24 August 2023.

[37] Eirini Ntoutsi, P. Fafalios, U. Gadiraju, Vasileios Iosifidis, W. Nejdl, Maria-Esther Vidal, S. Ruggieri, F. Turini, S. Papadopoulos, Emmanouil Krasanakis, I. Kompatsiaris, K. Kinder-Kurlanda, Claudia Wagner, F. Karimi, Miriam Fernández, Harith Alani, Bettina Berendt, Tina Kruegel, C. Heinze, Klaus Broelemann, G. Kasneci, T. Tiropanis and Steffen Staab. "Bias in data driven artificial intelligence systems—An introductory survey." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10 (2020). https://doi.org/10.1002/widm.1356. accessed 26 August 2024.

[38] Reconsidering the regulation of facial recognition in public spaces, Sara Solarova, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9274635/ accessed 24 August 2023.

[39] Emily Jones. "Digital disruption: artificial intelligence and international trade policy." Oxford Review of Economic Policy (2023). https://doi.org/10.1093/oxrep/grac049. accessed 26 August 2024.

[40] Jonathan W. Z. Lim and V. Thing. "Toward a Universal and Sustainable Privacy Protection Framework." Digital Government: Research and Practice, 4 (2023): 1 - 13. https://doi.org/10.1145/3609801. accessed 26 August 2024.

[41] Rainer Mühlhoff and Theresa Willem. "Social media advertising for clinical studies: Ethical and data protection implications of online targeting." Big Data & Society, 10 (2023). https://doi.org/10.1177/20539517231156127. accessed 26 August 2024.

[42] Privacy and artificial intelligence: challenges for protecting health information in a new era, Blake Murdoch, https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-021-00687-3 accessed 24 August 2023.

[43] CH.E.N. Sai Priya and Manas Kumar Yogi. "Trustworthy AI Principles to Face Adversarial Machine Learning: A Novel Study." September 2023 (2023). https://doi.org/10.36548/jaicn.2023.3.002. accessed 26 August 2024

privacy.[44]

1.4.1 The Issue of Bias and Discrimination

Bias and discrimination are significant privacy challenges in the age of AI that arise due to the use of biassed data and algorithms in AI systems.[45] In the era of AI, privacy faces significant challenges related to bias and discrimination. These issues stem from the use of biassed data and algorithms in AI systems, resulting in far-reaching consequences that impact privacy and exacerbate social inequalities.[46] This section explores how bias and discrimination manifest as critical privacy challenges within AI.

AI systems rely on vast datasets for training, but when these datasets carry biases, AI systems can perpetuate societal prejudices. Biases may originate from historical discrimination, cultural biases, or underrepresentation of certain groups.[47] Consequently, AI outputs can become inaccurate and unjust, raising concerns about fairness and privacy.

Bias and discrimination have a notable impact on automated decision-making in areas like hiring, lending, and law enforcement.[48] Biased algorithms can influence these decisions, leading to privacy violations for individuals in specific demographic groups. Unauthorised use of personal data, skewed by biassed algorithms, compounds the issue, causing harm to affected individuals and highlighting the intersection of bias, discrimination, and privacy infringement.[49] The opacity of many AI algorithms, especially complex deep learning models, poses a challenge in identifying and understanding sources of bias.[50] This lack of transparency hampers efforts to rectify and prevent discriminatory outcomes, hindering the development of fair and privacy-preserving AI.

Biassed AI systems can lead to unintentional privacy breaches, disproportionately affecting certain groups.[51] For example, biassed facial recognition systems may misidentify individuals, compromising their privacy.[52] These misidentifications underscore the interplay between bias, discrimination, and privacy concerns.

Discriminatory AI systems can exacerbate societal inequalities, fostering exclusion among specific demographics.[53] This exclusion not only limits opportunities and access to services but also raises privacy concerns for those subjected to discrimination.[54]

Biassed AI systems compromise the principles

[44] M. Bielova and D. Byelov. "Challenges and threats of personal data protection in working with artificial intelligence." Uzhhorod National University Herald. Series: Law (2023). https://doi.org/10.24144/2307-3322.2023.79.2.2. accessed 26 August 2024.

[45] AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry, Lorenzo Belenguer, https://link.springer.com/article/10.1007/s43681-022-00138-8 accessed 24 August 2023.

[46] Emilio Ferrara. "Fairness And Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, And Mitigation Strategies." ArXiv, abs/2304.07683 (2023). https://doi.org/10.48550/arXiv.2304.07683. accessed 26 August 2024.

[47] Lakshitha R Jain and Vineetha Menon. "AI Algorithmic Bias: Understanding its Causes, Ethical and Social Implications." 2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI) (2023): 460-467. https://doi.org/10.1109/ICTAI59109.2023.00073. accessed 26 August 2024.

[48] Sihang Li, Kuangzheng Li and Haibing Lu. "National Origin Discrimination in Deep-learning-powered Automated Resume Screening." ArXiv, abs/2307.08624 (2023). https://doi.org/10.48550/arXiv.2307.08624. accessed 26 August 2024.

[49] M. Bielova and D. Byelov. "Challenges and threats of personal data protection in working with artificial intelligence." Uzhhorod National University Herald. Series: Law (2023). https://doi.org/10.24144/2307-3322.2023.79.2.2. accessed 26 August 2024.

[50] Jason Liartis, Edmund Dervakos, Orfeas Menis-Mastromichalakis, A. Chortaras and G. Stamou. "Searching for explanations of black-box classifiers in the space of semantic queries." Semantic Web (2023). https://doi.org/10.3233/sw-233469. accessed 26 August 2024.

[51] Abdul Majeed and Seong Oun Hwang. "When AI Meets Information Privacy: The Adversarial Role of AI in Data Sharing Scenario." IEEE Access, 11 (2023): 76177-76195. https://doi.org/10.1109/ACCESS.2023.3297646. accessed 26 August 2024.

[52] Latika Kharb and Deepak Chahal. "Privacy Threats in Facial Recognition-Based Identity Verification." International Journal of Advanced Research in Science, Communication and Technology (2023). https://doi.org/10.48175/ijarsct-11686. accessed 26 August 2024.

[53] Ondrej Bohdal, Timothy M. Hospedales, Philip H. S. Torr and Fazl Barez. "Fairness in AI and Its Long-Term Implications on Society." ArXiv, abs/2304.09826 (2023). https://doi.org/10.48550/arXiv.2304.09826. accessed 26 August 2024.

[54] ibid

of consent and control over personal data. The secretive decision-making process within these systems deprives individuals of informed consent and control over their information, highlighting the connection between bias, lack of consent, diminished control, and compromised privacy.[55]

The lasting impacts of biassed AI systems are perpetuated through feedback loops that solidify existing biases.[56] For instance, biassed hiring algorithms may perpetuate underrepresentation of certain demographics in the workforce.[57] This cycle exacerbates inequalities and underscores the complex interplay between bias, discrimination, and the erosion of privacy.

The intricate challenges of bias and discrimination are deeply intertwined with AI's privacy landscape, necessitating comprehensive mitigation strategies to ensure equitable, unbiased, and privacy-respecting AI systems in the modern era.

1.4.2 The Issue of Job Displacements for Workers

Job displacement in the age of AI presents a multifaceted privacy challenge driven by interconnected factors.[58] One key aspect is the exposure of sensitive employment data as automation and AI technologies reshape job functions.[59] This goes beyond employment shifts, involving personal information like job evaluations and financial details. Inadequate privacy measures during data processing could adversely impact both personal and professional aspects of workers' lives.[60]

Moreover, the involvement of third-party service providers in AI-based transitions introduces the risk of data breaches and unauthorised sharing.[61] The lack of stringent data protection protocols amplifies vulnerability to breaches, potentially exposing private worker information to unauthorised entities, with far-reaching consequences.[62]

The role of AI algorithms in job retention decisions adds complexity. Lack of transparency and explainability in these algorithms leaves workers in the dark about the rationale behind their displacements, raising concerns about both fairness and privacy.[63] Biases in historical employment data can also be perpetuated, fostering discriminatory practices that infringe

[55] O. Olena. "Political and Legal Implications of the Use of Artificial Intelligence." Yearly journal of scientific articles "Pravova derzhava" (2023). https://doi.org/10.33663/1563-3349-2023-34-684-693. accessed 26 August 2024.

[56] Emilio Ferrara. "The Butterfly Effect in Artificial Intelligence Systems: Implications for AI Bias and Fairness." SSRN Electronic Journal (2023). https://doi.org/10.2139/ssrn.4614234. accessed 26 August 2024.

[57] Ondrej Bohdal, Timothy M. Hospedales, Philip H. S. Torr and Fazl Barez. "Fairness in AI and Its Long-Term Implications on Society." ArXiv, abs/2304.09826 (2023). https://doi.org/10.48550/arXiv.2304.09826. accessed 26 August 2024.

[58] Amogh Amol Karangutkar. "The Impact of Artificial Intelligence on Job Displacement and the Future of Work." International Journal of Advanced Research in Science, Communication and Technology (2023). https://doi.org/10.48175/ijarsct-12096. accessed 26 August 2024.

[59] Prajot Modhoriye, Pratik Yadav and Dr. Sarika Jadhav. "AI Transformation in Business: Unveiling the Dual Effects of Advancement and Challenges." INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (2023). https://doi.org/10.55041/ijsrem27359. accessed 26 August 2024.

[60] Adrienne Komanovics. "WORKPLACE PRIVACY IN THE EU : THE IMPACT OF EMERGING TECHNOLOGIES ON EMPLOYEE'S FUNDAMENTAL RIGHTS." EU and comparative law issues and challenges series (2023). https://doi.org/10.25234/eclic/27458. accessed 26 August 2024.

[61] Md Mostafizur Rahman, Aiasha Siddika Arshi, Md. Golam Moula Mehedi Hasan, Sumayia Farzana Mishu, H. Shahriar and Fan Wu. "Security Risk and Attacks in AI: A Survey of Security and Privacy." 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC) (2023): 1834-1839. https://doi.org/10.1109/COMPSAC57700.2023.00284. accessed 26 August 2024.

[62] Prashant Manuja, R. Shekhawat and U. Rawat. "Design & analysis of novel IT security framework for overcoming data security & privacy challenges." Journal of Discrete Mathematical Sciences & Cryptography (2023). https://doi.org/10.47974/jdmsc-1776. accessed 26 August 2024.

[63] Alejandro Pena, Ignacio Serna, A. Morales, Julian Fierrez, Alfonso Ortega, Ainhoa Herrarte, Manuel Alcántara and J. Ortega-Garcia. "Human-Centric Multimodal Machine Learning: Recent Advances and Testbed on AI-Based Recruitment." SN Computer Science, 4 (2023). https://doi.org/10.1007/s42979-023-01733-0. accessed 26 August 2024.

on privacy and equal opportunities.[64]

Workers often lack control over their personal information during job displacement, with data used and shared beyond their control, eroding trust in data management.[65] Post-displacement, the retention of workers' data without clear justification poses a privacy concern, especially when individuals remain unaware of how their information is being used.[66]

1.4.3 The Issue of Data Abuse Practices

In the current era dominated by AI-driven technologies, the issue of data abuse has become a significant challenge to privacy. As AI continues to advance and permeate various sectors, the risk of data abuse has grown substantially, carrying profound consequences for both individuals and society as a whole.[67] This section explores key aspects of data abuse in the context of AI-driven data processing.

Data abuse often begins with unethical data collection practices. Some organisations collect personal data without obtaining explicit consent or resort to deceptive methods to acquire data.[68] Since AI systems heavily depend on vast datasets for optimal performance, unscrupulous data collection methods can lead to the covert accumulation of sensitive information without individuals' awareness or consent.[69]

Another troubling aspect of data abuse is the unauthorised monetization of data. Certain entities gather user data with the intention of selling or sharing it with third parties, disregarding individuals' knowledge or consent.[70] This practice severely violates user privacy and their ability to control their personal information.

AI-driven data processing enables intricate profiling capabilities. By analysing online activities, preferences, and behaviours, AI can create detailed profiles of individuals.[71] These profiles may then be exploited to generate targeted content or advertisements, potentially manipulating user decisions and behaviour without their knowledge.[72]

Algorithmic discrimination, while often unintentional, is another worrisome outcome of AI algorithms. These algorithms can inherit biases from their training data, perpetuating discriminatory practices such as biassed hiring, unequal loan approvals, or prejudiced

[64] C. Beasley and Y. J. Xiao. “Incarceration history and ethnic bias in hiring perceptions: An experimental test of intersectional bias & psychological mechanisms.” PLOS ONE, 18 (2023). https://doi.org/10.1371/journal.pone.0280397. accessed 26 August 2024.

[65] Haleh Asgarinia, Andrés Chomczyk Penedo, Beatriz Esteves and David Bruce Lewis. “”Who Should I Trust with My Data?” Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies.” Inf., 14 (2023): 351. https://doi.org/10.3390/info14070351. accessed 26 August 2024.

[66] Dan Calacci and Jake M L Stein. “From access to understanding: Collective data governance for workers.” European Labour Law Journal, 14 (2023): 253 - 282. https://doi.org/10.1177/20319525231167981. accessed 26 August 2024.

[67] Y. Bengio, Geoffrey Hinton, Andrew Yao, Dawn Song, Pieter Abbeel, Y. Harari, Ya-Qin Zhang, Lan Xue, S. Shalev-Shwartz, Gillian Hadfield, Jeff Clune, Tegan Maharaj, Frank Hutter, Atilim Gunecs Baydin, Sheila McIlraith, Qiqi Gao, Ashwin Acharya, David Krueger, Anca Dragan, Philip Torr, Stuart Russell, Daniel Kahneman, J. Brauner and S. Mindermann. “Managing AI Risks in an Era of Rapid Progress.” ArXiv, abs/2310.17688 (2023). https://doi.org/10.48550/arXiv.2310.17688. accessed 26 August 2024.

[68] Thi Huyen Pham, Thuy-Anh Phan, Phuong-Anh Trinh, Xuan Bach Mai and Quynh-Chi Le. “Information security risks and sharing behavior on OSN: the impact of data collection awareness.” Journal of Information, Communication and Ethics in Society (2023). https://doi.org/10.1108/jices-06-2023-0076. accessed 26 August 2024.

[69] K. Kim. “Study on Artificial Intelligence(AI) and Chat GPT, Corruption.” The Korea Association for Corruption Studies (2023). https://doi.org/10.52663/kcsr.2023.28.2.85. accessed 26 August 2024.

[70] F. Jaber and M. Abbad. “A realistic evaluation of the dark side of data in the digital ecosystem.” Journal of Information Science (2023). https://doi.org/10.1177/01655515231205499. accessed 26 August 2024.

[71] Yeqing Kong and Huiling Ding. “Tools, Potential, and Pitfalls of Social Media Screening: Social Profiling in the Era of AI-Assisted Recruiting.” Journal of Business and Technical Communication, 38 (2023): 33 - 65. https://doi.org/10.1177/10506519231199478. accessed 26 August 2024.

[72] Swati Sharma Et al.. “Ethical Considerations in AI-Based Marketing: Balancing Profit and Consumer Trust..” Tuijin Jishu/Journal of Propulsion Technology (2023). https://doi.org/10.52783/tjjpt.v44.i3.474. accessed 26 August 2024.

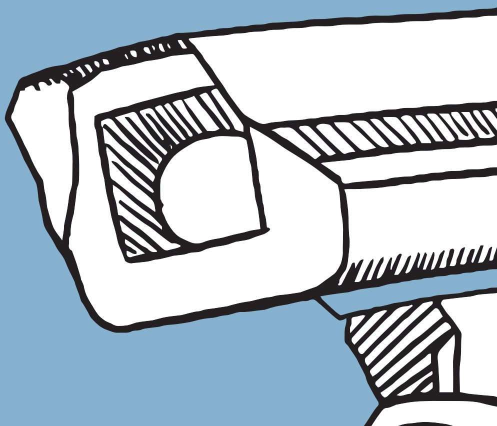
law enforcement profiling.[73] Such actions disproportionately affect specific demographic groups and impinge on their privacy rights.

Excessive data retention, a facet of data abuse, can be observed in AI systems storing more data than necessary for their intended purpose. This excessive accumulation increases the risk of unauthorised data access and breaches, jeopardising the privacy of individuals connected to the data.[74]

The vulnerability of personal data is further exacerbated by mishandling and inadequate security measures. Insufficient precautions can lead to data breaches and leaks, leaving personal information susceptible to misuse and exploitation.[75]

AI-generated misinformation, exemplified by deepfake content, poses a potent threat. These convincing fabrications, including videos and audio, can be used to disseminate false information, influence public opinion, and compromise both privacy and reputation.[76]

An interconnected concern involves cross-referencing data from diverse sources. AI systems can amalgamate data fragments to construct comprehensive individual profiles, potentially revealing sensitive information that individuals



[73] Aislinn Kelly-Lyth. “Algorithmic discrimination at work.” European Labour Law Journal, 14 (2023): 152 - 171. https://doi.org/10.1177/20319525231167300. accessed 26 August 2024.
[74] Hüseyin Ensari Eryılmaz. “Personal Data Privacy in the Age of Artificial Intelligence.” TSBS Bildiriler Dergisi (2023). https://doi.org/10.55709/tsbsbildirilerdergisi.539. accessed 26 August 2024.
[75] Abhishek Pant. “Importance of Data Security and Privacy Compliance.” International Journal for Research in Applied Science and Engineering Technology (2023). https://doi.org/10.22214/ijraset.2023.56862. accessed 26 August 2024.
[76] Mohamed R. Shoaib, Ze Wang, Milad Taleby Ahvanooey and Jun Zhao. “Deepfakes, Misinformation, and Disinformation in the Era of Frontier AI, Generative AI, and Large AI Models.” ArXiv, abs/2311.17394 (2023). https://doi.org/10.48550/arXiv.2311.17394. accessed 26 August 2024.

> An interconnected concern involves cross-referencing data from diverse sources. AI systems can amalgamate data fragments to construct comprehensive individual profiles, potentially revealing sensitive information that individuals are unwilling to share voluntarily.

are unwilling to share voluntarily.[77] This practice exacerbates the complex web of data abuse issues perpetuated by AI technologies.

In the context of data protection and privacy, Kenya has taken significant steps to address these concerns. In 2019, Kenya introduced its Data Protection law, primarily aimed at safeguarding personal data and empowering individuals with rights over their information.[78] This law encompasses both automated and non-automated data processing. The appointment of the Data Protection Commissioner, mandated by this law, occurred in 2020. To operationalize the Data Protection Act and the Commissioner's role, regulations were enacted in 2022. These regulations comprise the Data Protection (General) Regulations 2021[79], the Data Protection (Compliance and Enforcement) Regulations, 2021[80], and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021[81]. These legal developments have established a framework for privacy and data protection in Kenya, prompting organisations to adapt by registering as data controllers and processors. Notably, even the Central Bank of Kenya Act[82] underwent revisions to mandate the registration of digital lending apps with the ODPC, ensuring compliance as a prerequisite for obtaining a business licence from the Central Bank.[83]

However, despite organisations initially complying by registering as data handlers, some have not demonstrated a commitment to adhere to the Data Protection Act beyond this point.[84] Regrettably, certain actions by organisations, including government entities, have blatantly violated the Act's provisions. In May 2022, the Kenya Revenue Authority (KRA) announced plans to deploy software to extract data from taxpayers' digital devices to combat tax fraud.[85] This, along with proposed amendments to the Huduma Namba Bill, allowing KRA access to sensitive taxpayer data in the National Integrated Identity Management System (NIIMS) database, clearly infringes upon citizens' privacy

[77] D. Zha, Zaid Pervaiz Bhat, Kwei-Herng Lai, Fan Yang, Zhimeng Jiang, Shaochen Zhong and Xia Hu. "Data-centric Artificial Intelligence: A Survey." ArXiv, abs/2303.10158 (2023). https://doi.org/10.48550/arXiv.2303.10158. accessed 26 August 2024.

[78] Data Protection Act, 2019 (Act No.24 of 2019).

[79] The Data Protection (General) Regulations, 2021.

[80] The Data Protection (Compliance and Enforcement) Regulations, 2021.

[81] The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

[82] The Central Bank of Kenya Act, 1966 (Chapter 491 of the Laws of Kenya).

[83] Mondaq 'Kenya: Data Protection Registration Law Comes into Force on July 14, 2022' (2022) https://www.mondaq.com/data-protection/1216300/data-protection-registration-law-comes-into-force-on-14-july-2022 accessed on 12 September 2023.

[84] KICTANet 'Data Protection, Three Years Later - The Good, The Bad, and The Ugly' (2022) https://www.kictanet.or.ke/data-protection-three-years-later-the-good-the-bad-and-the-ugly/ accessed on 12 September 2023.

[85] QUARTZ 'Kenyans Are Protesting Plans by Tax Authority to Snoop on Their Online Chats' (2022) https://qz.com/africa/2164861/kenyas-tax-authority-to-snoop-on-online-chats-to-combat-fraud accessed on 12 September 2023.

and data protection rights.[86] In late 2022, the Communications Authority of Kenya advocated for the installation of surveillance tools on mobile phone networks under the Device Management Systems policy to detect counterfeit mobile phones often used in criminal activities.[87] Safaricom, a leading telecom provider, contested this move, citing concerns about user privacy and third-party access to subscriber data.[88]

During the recent election, the Independent Electoral and Boundaries Commission (IEBC), constitutionally responsible for overseeing elections in Kenya, exhibited questionable data protection practices, as observed by the ICT think tank, KICTANet.[89] Among the noted concerns were the development of an Election Guidance Note to instruct data controllers and processors on handling voter data.[90] However, the Commission failed to disclose its purported Data Protection Impact Assessment and privacy policy.[91]

In early 2022, Safaricom, Kenya's leading telecom provider, faced a class-action lawsuit for breaching the privacy rights of its subscribers. In this legal action, it was revealed that two of the telco's employees had unlawfully leaked the data of millions of subscribers and distributed it to unauthorised parties, in clear violation of the Data Protection Act.[92] These instances highlight the ongoing challenges and complexities surrounding data protection and privacy in Kenya's evolving digital landscape.

[86] Paradigm Initiative Network, 'LONDA 2022 Digital Rights and Inclusion in Africa Report- Kenya' https://paradigmhq.org/wp-content/uploads/2023/06/Kenya-Londa-2022.pdf accessed on 12 September 2023.

[87] The Centre for Intellectual Property and Information Technology Law, "Unpacking the Device Management System (DMS) Judgement," https://cipit.strathmore.edu/unpacking-the-device-management-system-dms-judgement-2/ accessed on 12 September 2023.

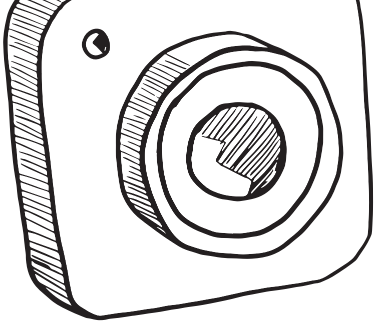
[88] ibid.

[89] KICTANet 'Safeguarding Personal Data During Kenya's 2022 General Elections' (2022) https://www.kictanet.or.ke/safeguarding-personal-data-during-kenyas-2022-general-election/ accessed on 12 September 2023.

[90] ibid

[91] ibid.

[92] Twitter 2021 post, https://web.archive.org/web/20210207124248/https://twitter.com/KinyanBoy/status/1358395467462279175 accessed 12 September 2023.



2.0 Kenya's Digital Transformation and AI Policy Landscape

Kenya is making significant strides in positioning itself within the digital economy, despite the absence of a formal national AI strategy. In 2018, the Kenyan government established a Blockchain and AI task force to explore the potential of these emerging technologies.[93] This task force delved into various applications of AI, including public service enhancement, financial inclusion, cybersecurity, and election processes. It identified three primary areas for AI development: fighting corruption, strengthening the financial sector, and improving the transparency of elections to bolster democracy.[94] However, these recommendations have yet to translate into concrete policies or legislation.

Kenya unveiled its Digital Economy Blueprint in 2019, aligning with the broader Digital Economy Blueprint for Africa.[95] This blueprint delineated six key pillars for the country's digital economy ecosystem: Digital Government, Digital Business, Infrastructure, Innovation-Driven Entrepreneurship and Digital Skills, and Values and Digital Inclusion.[96] Furthermore, Kenya adopted the Digital Economy Strategy 2020, prioritising digital infrastructure, business innovation, education, skills development, technology transfer, and commercialization.[97] These initiatives aim to address OECD AI principles, such as fostering an inclusive digital ecosystem, promoting sustainable development, ensuring transparency, and enabling an environment conducive to AI.

In April 2022, Kenya introduced the Kenya Digital Master Plan (DMP) 2022-2032, building upon previous master plans.[98] This comprehensive blueprint identifies 20 flagship programs, spanning digital infrastructure, government services, digital skills, and digital enterprises, alongside an overarching policy, legal, and regulatory framework. It signifies Kenya's commitment to embracing AI as a cornerstone

[93] Judy Kabubu. Official Intelligence in Kenya, (Jan 26, 2021) https://mman.co.ke/content/artificial-intelligence-ai-kenya accessed on 12 September 2023.
[94] Kenn Abuya, Kenya Blockchain Task Force Findings Rally for Use Cases in Poll Transparency, Teckweez (Jul 26, 2019), https://techweez.com/2019/07/26/blockchaintaskforce-report/ accessed on 12 September 2023.
[95] Ministry of ICT, Innovation and Youth Affairs. Kenya Digital Economy Blueprint 2019, p. 96. https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy2019.pdf accessed on 12 September 2023.

[96] OECD.AI. Kenya's Digital Economy Blueprint.\ 2019 https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F-2021data-policyInitiatives-27137 accessed on 12 September 2023.
[97] Ministry of Information, Communication, TechnologyICT, Innovation and Youth Affairs, Digital Economy Strategy 2020, 2020. (Jul 10, 2020). https://ict.go.ke/wpcontent/uploads/2020/08/10TH-JULY-FINAL-COPY-DIGITAL-ECONOMYSTRATEGY-DRAFT-ONE.pdf. accessed on 12 September 2023.
[98] U.S. International Trade Administration, Kenya launches new ten-year digital masterplan (Jun 13, 2022), https://www.trade.gov/market-intelligence/kenya-launchesnew-ten-year-digital-masterplan accessed on 12 September 2023.

of its digital future.[99]

Kenya actively collaborates with international organisations and stakeholders to align its AI policies with broader continental goals. As a member of the African Union (AU), Kenya is dedicated to developing human-centred AI policies in accordance with the AU's digital transformation strategy and the Continental Data Policy Framework.[100] The AU AI Working Group fosters collaboration among African states, aiming to develop AI strategies, address regulatory challenges, and learn from regional best practices.[101]

Kenya has also made significant investments in AI research and development, with an accumulated investment of Sh13 billion (US$120 million) over the past decade.[102] Initiatives like the Digital Literacy Programme and research grants for AI applications highlight Kenya's commitment to AI development and capacity building.[103]

Kenya has established a systematic process for public participation in policy-making through the Public Consultation portal of the Communications Authority of Kenya.[104] This approach ensures that various stakeholders have a say in shaping regulatory sandboxes and other initiatives, promoting inclusivity and transparency.

In November 2019, Kenya passed the Data Protection Act (DPA), which aimed to safeguard personal data and uphold the right to privacy, aligning with Article 31(c) and (d) of the Constitution.[105] This legislation sought to regulate the processing of personal data, define data subjects' rights, and impose responsibilities on data controllers and processors. The DPA's relevance to AI becomes evident when personal data is involved in AI transactions. It encompasses data protection principles like fair and transparent data processing, erasure and rectification rights, and rights related to automated decision-making.

In response to the DPA, the Office of the Data Protection Commissioner (ODPC) was established in 2020 and joined the Global Privacy Assembly (GPA) in 2022, connecting with over 130 data protection authorities worldwide.[106] However, the ODPC has not endorsed several GPA declarations and resolutions related to ethics, AI, and facial recognition technology such as the 2018 GPA Declaration on Ethics and Data Protection, the GPA 2020 Resolution on Accountability in the Development and Use of AI and the GPA 2022 Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology.[107]

Kenya introduced additional regulations in 2021 and 2022 to enhance privacy and support its digital economy, including measures to address unethical debt collection practices and digital

[99] Ministry of ICT, Innovation and Youth Affairs. The Kenya National Digital Master Plan 2022-2032 (Apr, 2022), https://repository.kippra.or.ke/bitstream/handle/123456789/3580/Kenya%20%20Digital%20Master%20Plan.pdf?sequence=1&isAllowed=y accessed on 12 September 2023.

[100] African Union, The Digital Transformation Strategy for Africa (2020-2030), https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf accessed on 12 September 2023.

[101] F Ngila Kenya, Africa Hurdles in Artificial Intelligence Race, Business Daily (Jan 7, 2021), https://www.businessdailyafrica.com/bd/corporate/technology/kenya-africahurdles-in-artificial-intelligence-race-3249180 accessed on 12 September 2023.

[102] Faustine Ngila, Kenya, Africa Hurdles in Artificial Intelligence Race Business Daily (Jan 7, 2021), https://www.businessdailyafrica.com/bd/corporate/technology/kenyaafrica-hurdles-in-artificial-intelligence-race-3249180 accessed on 12 September 2023.

[103] OECD.AI Policy Observatory, AI in Kenya, Kenya's Digital Literacy Programme (Digischool) (Aug. 11, 2021), https://oecd.ai/en/dashboards/policyinitiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27139 accessed on 12 September 2023.

[104] Communications Authority of Kenya, Public Consultation, https://www.ca.go.ke/?taxonomy=consultation&s=&document_category=consultation accessed on 12 September 2023.

[105] Constitution of Kenya 2010 art. 31 (c) & (d).

[106] Global Privacy Assembly, 44th Closed Session of the Global Privacy Assembly (Oct.27, 2022), https://globalprivacyassembly.org/wp-content/uploads/2022/11/1.1.-b.-GPA2022-Accreditation-Resolution.pdf accessed 12 September 2023.

[107] Center for AI and Digital Policy, Artificial Intelligence and Democratic Values 2022, https://www.caidp.org/reports/aidv-2022/ accessed 12 September 2023.

Kenya's active engagement with AI-related initiatives and its commitment to developing a comprehensive AI strategy demonstrate its dedication to the digital transformation.

credit provider regulations.[108] Despite the African Union's development of the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), Kenya has not signed or ratified it, leading to calls for its adoption to promote regional cooperation.[109]

Section 22 of the Data Protection Act highlights algorithmic transparency, requiring data controllers and processors to inform data subjects about automated individual decision-making and provide meaningful information about the underlying logic.[110] However, concerns emerged regarding the use of government-endorsed educational technology tools for online learning during the COVID-19 pandemic, raising questions about children's privacy rights.[111]

Given the growing issue of algorithmic discrimination, Kenya may need comprehensive non-discrimination legislation to address associated risks.[112] The country's Ministry of Education also faced public scrutiny regarding automated decision-making in admission processes, emphasising the importance of transparency in such systems.[113]

Kenya initiated biometric registration efforts, including the Huduma Namba project, which raised privacy concerns and challenges from digital rights groups.[114] On the 29th of September, the government issued an official press statement indicating the postponement of the forthcoming inauguration of the Maisha Namba and Digital ID ecosystem, initially slated for October 2, 2023, under the auspices of His Excellency President William Ruto. A revised launch date will be communicated in due course. Concurrently, the process of soliciting public input and engaging with stakeholders concerning the Maisha Namba and Digital ID ecosystem is actively progressing across the nation. The Maisha Card is set to take over the role of the national ID card and will also serve as the identifier for death registration. Additionally, digital signatures will be recognized as a means of confirming one's identity during mobile transactions. The population register

[108] ibid.

[109] African Union, List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection (Mar. 25, 2022), https://au.int/sites/default/files/treaties/29560-slAFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf accessed 12 September 2023.

[110] Data Protection Act No.24 of 2019 s.22.

[111] Human Rights Watch, How Dare They Peep into My Private Life? (May 25, 2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrensrights-violations-governments accessed 12 September 2023.

[112] CEGA, Manipulation-proof credit scoring algorithms in Kenya (2023), https://cega.berkeley.edu/research/building-better-credit-scoring-algorithms/ accessed 12 September 2023.

[113] Frankline Nkonge, Legal Challenges facing algorithmic decision-making in Kenya (Oct 2021), https://www.researchgate.net/publication/355169613_LEGAL_CHALLENGES_FACING_ALGORITHMIC_DECISION-MAKING_IN_KENYA accessed 12 September 2023.

[114] Ayang Macdonald, Kenya mulls digital ID scheme changes and new uses for controversial Huduma Namba (Jan. 16, 2023), https://www.biometricupdate.com/202301/kenya-mulls-digital-id-scheme-changes-andnew-uses-for-controversial-hudumanamba#:~:text=The%20Huduma%20Namba%20biometric%20ID,been%20stuck%20in%20Kenya's%20parliament accessed 12 September 2023.

will undergo integration, consolidating Kenya's current databases encompassing both citizens and refugees. Additionally, the introduction of biometric passports in 2022 further highlights the country's efforts in identity management.[115]

Regarding facial recognition, the Kenyan National Police Service launched a system in 2018 to detect vehicles involved in crimes through CCTV cameras and Automatic Number Plate Recognition (ANPR).[116] Plans for an upgrade involve using facial recognition technology, called NeoFace, to identify suspects quickly.[117] This technology will analyse faces in real-time through thousands of cameras, complementing traditional fingerprint identification methods.[118]

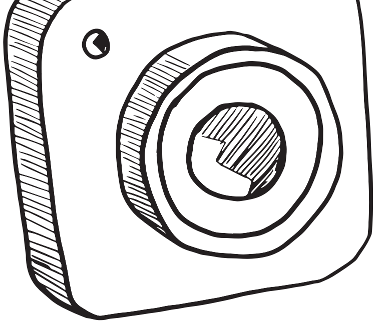
Kenya's active engagement with AI-related initiatives and its commitment to developing a comprehensive AI strategy demonstrate its dedication to the digital transformation. However, challenges such as privacy and algorithmic transparency require further attention to align with global best practices and principles.

[115] Ayang Macdonald, Kenya to clear backlog of biometric passports, new 'smart and digital ID' system coming. Biometric Update (Feb 6, 2023), https://www.biometricupdate.com/202302/kenya-to-clear-backlog-of-biometricpassports-new-smart-and-digital-id-system-coming accessed 12 September 2023.

[116] Chris Burt, Kenyan police launch facial recognition on urban CCTV network. Biometric Update (Sep 24, 2018), https://www.biometricupdate.com/201809/kenyanpolice-launch-facial-recognition-on-urban-cctv-network accessed 12 September 2023.

[117] Paul Wanjama, Police launch facial recognition system to nab criminals (Sept. 18, 2018), https://www.biometricupdate.com/201809/kenyan-police-launch-facialrecognition-on-urban-cctv-network accessed 12 September 2023.

[118] ibid



3.0 African Approaches to Protecting Privacy in the Age of AI

In the African context, addressing privacy concerns in the age of AI requires a nuanced approach, considering the region's unique challenges and opportunities.[119] Data sovereignty in Africa is a critical aspect of establishing effective data governance frameworks that prioritise privacy by design. It emphasises the principle that data generated within a nation's borders should be regulated by that country's laws, thereby allowing for tailored protections that reflect local values and legal contexts. This approach can strengthen citizens' trust in data handling practices and encourage responsible data use, as highlighted in the African Union Data Policy Framework discussion on the need for harmonised governance frameworks that facilitate data flow while ensuring adequate safeguards.[120] The African Union's initiatives, such as the Convention on Cyber Security and Personal Data Protection, aim to create a unified regulatory environment that supports cross-border data transactions while protecting individual rights.[121]

However, the implementation of data sovereignty and governance in Africa faces significant challenges that can hinder the effectiveness of privacy by design. Many countries grapple with infrastructural deficiencies and limited technical expertise, which impede their ability to enforce data protection laws adequately.[122] Additionally, the reliance on foreign cloud services can complicate local governance efforts, as these services may not adhere to national regulations, leading to potential data exploitation.[123] To overcome these weaknesses, the document emphasises the importance of capacity-building initiatives and the integration of sector-specific guidelines into national data governance regimes.[124] By addressing these challenges, African nations can create a more robust framework for data protection that not only safeguards individual privacy but also fosters innovation and economic growth in the digital age.

Several global approaches and initiatives can provide valuable insights and frameworks to guide African countries in their efforts to enhance privacy and data protection in the realm of artificial intelligence. The General Data Protection Regulation (GDPR), although enacted by the European Union, has had a significant

[119] J. Zamaraeva and M. Kolesnik. "On the issue of cultural (African) specifics of "responsible artificial intelligence"." Asia, America and Africa history and modernity (2023). https://doi.org/10.31804/2782-540x-2023-2-1-43-75. accessed 26 August 2024.

[120] African Union Data Policy Framework, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf p.51 accessed 26 August 2024.

[121] ibid p.64

[122] ibid p.51

[123] ibid p.57

[124] ibid p.64

influence on global privacy standards.[125] Its emphasis on individual data rights, consent, and data protection principles serves as a valuable reference point for African nations as they work to strengthen their own privacy regulations. Drawing inspiration from GDPR can help African countries establish a solid foundation for data protection in AI contexts.[126] Africa is still heavily reliant on datasets from global north but AI surveillance is gaining traction in Africa with the policies and strategies in place.[127]

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework is another relevant initiative for African nations.[128] This framework prioritises principles such as individual autonomy, accountability, and proportionality in data processing. Aligning with these principles can guide African countries in crafting privacy regulations that resonate with their cultural and societal contexts while upholding fundamental data protection values.[129]

Participation in the Global Privacy Assembly offers African data protection authorities the opportunity to engage in discussions on privacy challenges and share best practices with their global counterparts.[130] This collaboration can be invaluable for shaping effective privacy policies and practices that suit the African context.

Privacy-Enhancing Technologies (PETs) hold great promise for bolstering data protection in Africa's AI landscape.[131] Integrating PETs into AI systems can help mitigate data exposure and reduce vulnerabilities associated with privacy breaches.[132] Embracing these technologies can enhance the overall privacy posture of AI applications in Africa.

Finally, promoting public awareness and education is paramount. African nations must empower individuals to make informed decisions about their privacy rights in the context of AI technologies.[133] Raising awareness about the functioning of AI systems and the importance of data protection practices is essential for building trust among users and fostering a culture of responsible AI usage.

[125] The General Data Protection Regulation, https://gdpr-info.eu/ accessed 12 September 2023.

[126] Lucas Hertzog, Jenny Chen-Charles, Camille Wittesaele, K. de Graaf, Ray Titus, Jane-Frances Kelly, N. Langwenya, L. Baerecke, B. Banougnin, W. Saal, John Southall, L. Cluver and E. Toska. "Data management instruments to protect the personal information of children and adolescents in sub-Saharan Africa." IASSIST Quarterly (2023). https://doi.org/10.29173/iq1044. accessed 26 August 2024.

[127] Aníbal Monasterio Astobiza, T. Ausín, Belén Liedo, M. Toboso, M. Aparicio and Daniel López. 'Ethical Governance of AI in the Global South: A Human Rights Approach to Responsible Use of AI.' The 2021 Summit of the International Society for the Study of Information (2022). https://doi.org/10.3390/proceedings2022081136. accessed 26 August 2024.

[128] Asia-Pacific Economic Cooperation (APEC) Privacy Framework, https://www.apec.org/publications/2005/12/apec-privacy-framework accessed 12 September 2023.

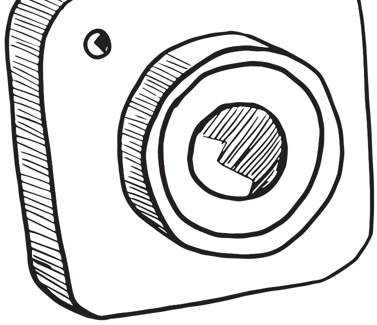
[129] Efe Lawrence-Ogbeide, Chiemeka Felix Nwosu and Olumide Babalola. "A Value Assessment of Personal Data: Towards Greater Privacy Consciousness in Africa." International Journal of Law and Society (2023). https://doi.org/10.11648/j.ijls.20230603.18. accessed 26 August 2024.

[130] Global Privacy Assembly, https://globalprivacyassembly.org/ accessed 12 September 2023.

[131] OECD, Emerging Privacy Enhancing Technologies, https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf-121be4-en.htm accessed 12 September 2023.

[132] Sakib Shahriar, Sonal Allana, Seyed Mehdi Hazratifard and Rozita Dara. "A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle." IEEE Access, 11 (2023): 61829-61854. https://doi.org/10.1109/ACCESS.2023.3287195. accessed 26 August 2024.

[133] Kazeem Ajasa Badaru and Ramashego Shila Mphahlele. "Effects of Emerging Technologies on African Development: A Narrative Review on Selected African Countries." Research in Social Sciences and Technology (2023). https://doi.org/10.46303/ressat.2023.19. accessed 26 August 2024.



4.0 Best Practices and mitigation measures for Privacy and Data Protection in AI

Sub-Saharan Africa is rapidly integrating AI technologies into various sectors, presenting both opportunities and challenges for privacy and data protection.[134] As the region embraces AI, it is essential to adopt best practices and mitigation measures tailored to its unique context.

Privacy by design should be foundational in AI projects from inception. Integrating privacy features into AI systems' architecture is vital to minimise risks to user data.[135] Furthermore, data minimization principles advise collecting only the necessary data essential for specific AI applications.[136] In practice, this means that AI initiatives, like mobile money services in Kenya, prioritise data security and minimise the collection of extraneous information, enhancing user trust.[137] Another example of this is seen in designing Namibia's digital-ID system that aims to build local trust and accountability, while considering global standards and balancing individual and community needs in data management.[138]

Obtaining informed consent is paramount before collecting and processing individuals' data. It involves clear explanations of how data will be used and providing easily understandable options for opting out.[139] Across Sub-Saharan Africa, initiatives in health tech, such as M-Tiba in Kenya, exemplify this practice.[140] Transparency in AI, especially in decision-making processes, empowers users by explaining data usage.[141] This is evident in South Africa's credit scoring systems, where users gain insights into how their financial information influences credit decisions, fostering accountability.[142]

[134] M. Achieng. "Digital Technologies for Integrated Food Loss and Waste Reduction in Agrifood Chains in Sub-Saharan Africa: A Scoping Review." 2023 IST-Africa Conference (IST-Africa) (2023): 1-11. https://doi.org/10.23919/IST-Africa60249.2023.10187757. accessed 26 August 2024.

[135] Md Mostafizur Rahman, Aiasha Siddika Arshi, Md. Golam Moula Mehedi Hasan, Sumayia Farzana Mishu, H. Shahriar and Fan Wu. "Security Risk and Attacks in AI: A Survey of Security and Privacy." 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC) (2023): 1834-1839. https://doi.org/10.1109/COMPSAC57700.2023.00284. accessed 26 August 2024.

[136] Abigail Goldsteen, Gilad Ezov, Ron Shmelkin, Micha Moffie and Ariel Farkash. "Data minimization for GDPR compliance in machine learning models." AI and Ethics (2021). https://doi.org/10.1007/s43681-021-00095-8. accessed 26 August 2024.

[137] A. Kingiri and Xiaolan Fu. "Understanding the diffusion and adoption of digital finance innovation in emerging economies: M-Pesa money mobile transfer service in Kenya." Innovation and Development, 10 (2019): 67 - 87. https://doi.org/10.1080/2157930X.2019.1570695. accessed 26 August 2024.

[138] S. Van Staden and N. Bidwell. "Localised Trust in a Globalised Knot: Designing Information Privacy for Digital-ID." ACM Journal on Computing and Sustainable Societies (2023). https://doi.org/10.1145/3616024. accessed 26 August 2024.

[139] R. Appiah. "Gurus and Griots: Revisiting the research informed consent process in rural African contexts." BMC Medical Ethics, 22 (2021). https://doi.org/10.1186/s12910-021-00659-7. accessed 26 August 2024.

[140] M-TIBA Privacy Policy, https://mtiba.com/privacy-policy/ accessed 26 August 2024.

[141] Dawood Ali MoDastoni. "Exploring methods to make AI decisions more transparent and understandable for humans." Advances in Engineering Innovation (2023). https://doi.org/10.54254/2977-3903/3/2023037. accessed 26 August 2024.

[142] KPMG, 'Southern Africa Banking Survey: Vision 2030,' https://assets.kpmg.com/content/dam/kpmg/za/pdf/2024/Southern%20Africa%20Banking%20Survey_Vision%202030%20final.pdf accessed 26 August 2024.

To protect user privacy, personal data should be anonymized or pseudonymized whenever possible.[143] These practices are crucial, especially in the region's mobile network services. For instance, mobile network providers aggregate location data for urban planning without revealing individual identities, maintaining data utility while preserving privacy.[144]

Conducting Privacy Impact Assessments (PIAs) and regular data protection audits helps identify potential risks and ensures adherence to privacy regulations.[145] In Sub-Saharan Africa, such assessments are essential in maintaining public trust in AI applications for public services, such as electoral processes.

Robust security measures for data storage and transfer are essential to safeguard sensitive information.[146] Encryption and secure protocols are widely employed in financial institutions and e-commerce platforms across the region, ensuring the confidentiality of user data.[147]
Regular evaluation of AI models for biases and fairness issues is necessary, particularly in applications like law enforcement in Rwanda.[148] This ensures that AI technologies do not perpetuate discriminatory outcomes and promote equitable access to justice.

Enhancing user control over their data, including easy access, modification, or deletion of personal information, is a cornerstone of privacy best practices across Sub-Saharan Africa.[149] Rigorous evaluation of third-party vendors for compliance with privacy and data protection standards is essential to uphold overall data integrity.[150] Continuous monitoring of AI systems is necessary to detect potential privacy issues or vulnerabilities, as demonstrated in the use of agricultural data analytics in Uganda.[151]

Fostering a culture of privacy within organisations begins with educating employees on privacy best practices, data protection policies, and the importance of safeguarding user data.[152] Staying current with relevant privacy regulations ensures compliance with laws and guidelines related to AI-driven data processing.

Empowering users with knowledge about their privacy rights and data usage builds trust, which is further strengthened by transparent communication of data practices and privacy policies.[153] As Sub-Saharan Africa increasingly adopts AI, these best practices and mitigation strategies are vital to unlocking AI's potential while safeguarding data privacy and ethical standards in the region.

[143] Yağmur Şahi n and I. Dogru. "An Enterprise Data Privacy Governance Model: Security-Centric Multi-Model Data Anonymization." Uluslararası Muhendislik Arastirma ve Gelistirme Dergisi (2023). https://doi.org/10.29137/umagd.1272085. accessed 26 August 2024.

[144] Joao C. Ferreira, Bruno Francisco, L. Elvas, Miguel Nunes and José A. Afonso. "Predicting People's Concentration and Movements in a Smart City." Electronics (2023). https://doi.org/10.3390/electronics13010096. accessed 26 August 2024.

[145] Dimitra Georgiou and C. Lambrinoudakis. "DPIA for Cloud-based Health Organizations in the context of GDPR." European Conference on Cyber Warfare and Security (2023). https://doi.org/10.34190/eccws.22.1.1144. accessed 26 August 2024.

[146] Chen Guo, Mohan Su and Fang Cui. "Research on Data Storage Security in Cloud Computing Environment." 2023 4th International Conference on Information Science, Parallel and Distributed Systems (ISPDS) (2023): 475-479. https://doi.org/10.1109/ISPDS58840.2023.10235362. accessed 26 August 2024.

[147] ibid

[148] The National AI Policy_ Rwanda https://www.minict.gov.rw/index.php?eID=dumpFile&t=f&f=67550&token=6195a53203e197ef-a47592f40ff4aaf24579640e accessed 12 September 2023.

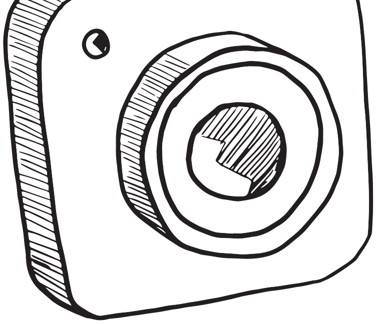
[149] S. Rennie, C. Atuire, T. Mtande, W. Jaoko, Sergio Litekwa, E. Juengst and K. Moodley. "Public health research using cell phone derived mobility data in sub-Saharan Africa: Ethical issues." South African Journal of Science (2023). https://doi.org/10.17159/sajs.2023/14777. accessed 26 August 2024.

[150] A-M.V. Tuz. "DATA PRIVACY AND SECURITY: LEGAL OBLIGATIONS FOR BUSINESSES IN THE DIGITAL AGE." Juridical scientific and electronic journal (2023). https://doi.org/10.32782/2524-0374/2023-6/150. Accessed 26 August 2024.

[151] Nalubega, T. & Uwizeyimana, D.E., 2024, 'Artificial intelligence technologies usage for improved service delivery in Uganda', Africa's Public Service Delivery and Performance Review 12(1), a770. https://doi.org/10.4102/apsdpr.v12i1.770 accessed 26 August 2024.

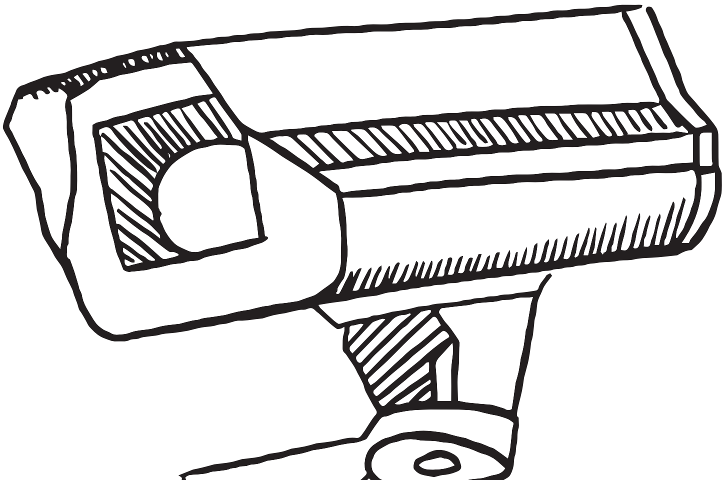
[152] Venessa Darwin and Mike Nkongolo. "Data Protection for Data Privacy-A South African Problem?." ArXiv, abs/2306.09934 (2023). https://doi.org/10.48550/arXiv.2306.09934. accessed 26 August 2024.

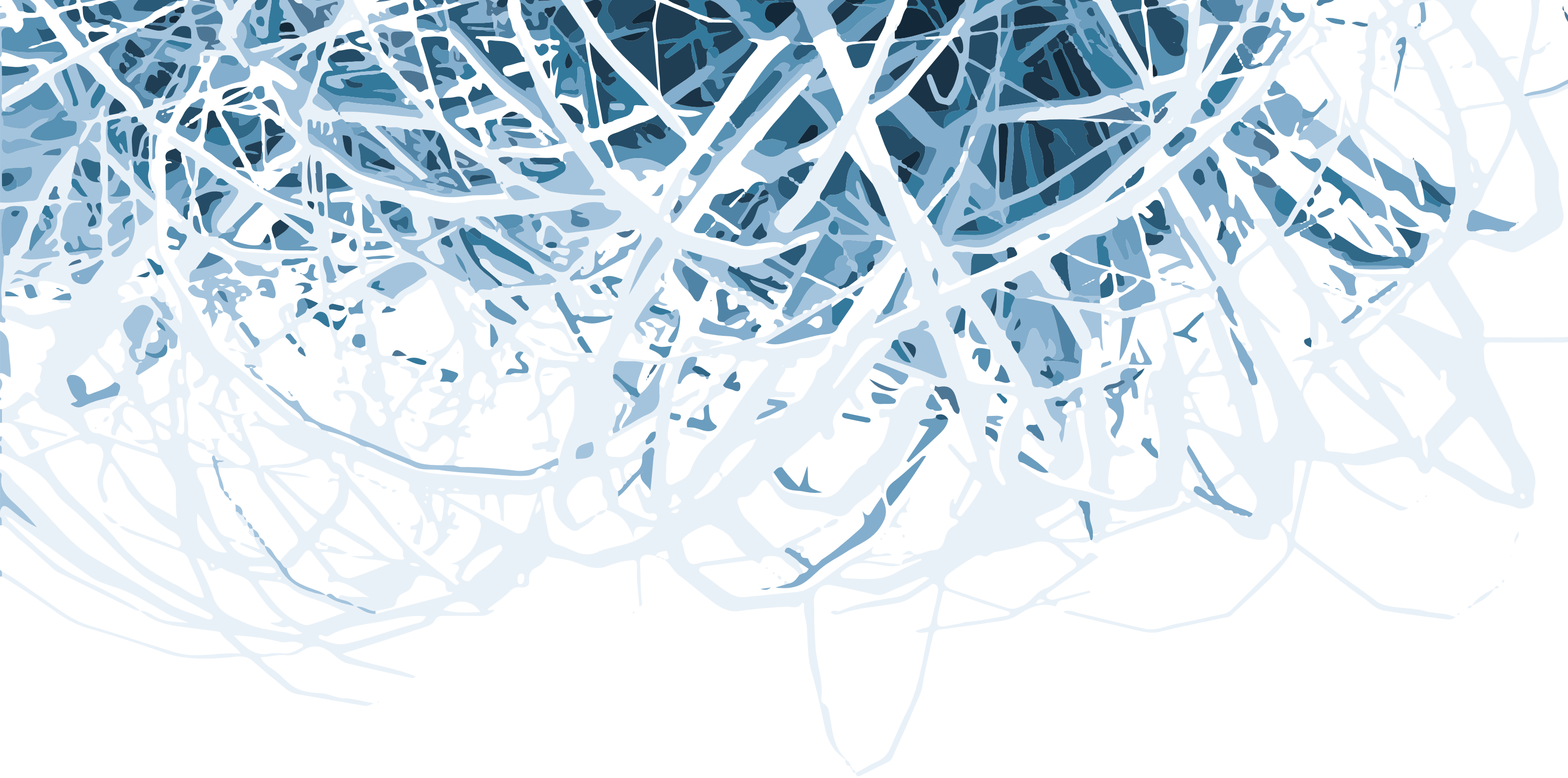
[153] Elias Grünewald, Johannes M. Halkenhäußer, Nicola Leschke and Frank Pallas. "Towards Cross-Provider Analysis of Transparency Information for Data Protection." ArXiv, abs/2309.00382 (2023). https://doi.org/10.48550/arXiv.2309.00382. accessed 26 August 2024.



5.0 Conclusion

In conclusion, as AI and surveillance technologies converge, safeguarding privacy becomes paramount. This report highlights the pivotal role of privacy in the digital era and examines its complex interplay with AI-driven data processing, job displacements, data abuse practices, and global approaches to protect privacy. For Sub-Saharan Africa, embracing AI requires tailored best practices to preserve privacy. Kenya's digital transformation shows promise but requires attention to privacy issues. African nations can draw from global initiatives, fostering public awareness to develop robust privacy frameworks. In the age of AI, privacy remains a fundamental right, demanding worldwide cooperation to protect individual autonomy, trust, and democratic values.





This study was made possible by a grant provided by the International Development Research Center (IDRC). We thank the organization for their continued support.

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

ARTIFICIAL INTELLIGENCE FOR DEVELOPMENT AFRICA

Sida
SWEDISH INTERNATIONAL
DEVELOPMENT COOPERATION AGENCY