AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: WK Mutuma 'Protecting human rights amid the rise of artificial intelligence surveillance in Africa' (2025) 25 *African Human Rights Law Journal* 777-800
http://dx.doi.org/10.17159/1996-2096/2025/v25n2a13

Protecting human rights amid the rise of artificial intelligence surveillance in Africa

Wyne Kenneth Mutuma[*]
Senior lecturer, School of Law, University of Nairobi, Kenya
https://orcid.org/0000-0002-1954-2702

Summary: *Artificial intelligence is the use of machines and computer systems to mimic human intelligence processes. In Africa, AI is already being used in domains such as health care, finance, manufacturing, law, transport, military technology and, now, specifically, surveillance technology. It is estimated that at least 14 states have already begun using smart policing and safe city initiatives to monitor their citizens and control criminal behaviour. The adoption of AI surveillance in Africa has been aided by increased investments and infrastructure-building efforts by foreign governments in Asia and Europe. The benefits of AI surveillance, especially in terms of reducing crimes such as terrorism, cannot be underestimated. However, there are concerns that the technology is not being procured or deployed in a transparent manner. Additionally, there are questions about how state actors process, store and use the large amounts of data collected using AI technology. There is growing concern that such data is being processed without legal and/or institutional checks and balances thereby resulting in human rights violations. For instance, there have been reports of AI surveillance being used in countries such as Uganda and Zambia to intercept the communications of political opponents. This article examines the extent of AI surveillance in Africa and its potential to become pervasive in the region, as well as the regulations that have been put in place to protect human rights (and the effectiveness thereof), especially privacy rights.*

[*] LLB (Liverpool) LLM PhD (Cape Town); wyne@uonbi.ac.ke

The article argues that the adoption of this revolutionary technology has not been accompanied by the necessary regulatory protections, with potentially negative impacts on fundamental rights. It therefore calls on states to scale up their efforts to ensure that human rights are safeguarded when using AI surveillance.

Key words: *artificial intelligence; surveillance technology; human rights; data privacy; Africa; digital governance; smart policing; regulatory frameworks*

1 Introduction

Numerous definitions have been advanced for the term 'artificial intelligence' (AI). Notably, being an evolving concept, there is no set meaning of the term. However, AI has been generally defined as 'the ability of machines and computer systems to simulate human intelligence processes such as learning, problem solving, planning and speech recognition'.[1] Surveillance, on the other hand, is the observation and collection of data to provide evidence for a purpose.[2] A clear distinction should be drawn between AI-enabled surveillance and traditional surveillance, as each carries different implications for privacy protection. Moreover, not all surveillance technologies deployed in Africa are AI-enabled. Surveillance without AI is typically limited to collecting and storing data. This data can then be analysed by humans to identify patterns or trends. However, this process can be time-consuming and labour-intensive. Surveillance with AI, on the other hand, can automatically analyse data and identify patterns or trends. This can be accomplished far more quickly and efficiently than through human analysis. However, AI-enabled surveillance also raises new privacy concerns, as it can be used to track and monitor people's activities in ways that were not before possible.

Through AI surveillance, governments can automate a variety of tracking and monitoring tasks, which also widens the scope of the surveillance network that may be cast.[3] The use of AI-based surveillance technologies has become an integral part of globalisation, resulting in a situation of, arguably, 'eyes everywhere,' although the distribution and intensity (the number of eyes and what they are able

[1] Z Saleh *Artificial intelligence definition, ethics and standards* (2019).

[2] *The law dictionary* (featuring *Black's law dictionary*), https://thelawdictionary.org/surveillance/#:~:text=SURVEILLANCE%20Definition%20%26%20Legal%20Meaning&text=Observation%20and%20collection%20of%20data%20to%20provide%20evidence%20for%20a%20purpose (accessed 10 November 2022).

[3] S Feldstein *The global expansion of AI surveillance* (2019) 13.

to see) varies from place to place, resulting in unique manifestations based on the circumstances in each context.[4]

AI surveillance technology is value neutral and does not in itself encourage unlawful use by states.[5] In practice, unless there is a motive to impose political repression or restrict individual liberties, official monitoring is not illegal and, therefore, may be properly conducted.[6] Thus, it has even been claimed that widespread targeted surveillance is both common and acceptable and is deeply ingrained in political, business and social organisations in several jurisdictions.[7] Nonetheless, public opinion regarding the need for surveillance is not unitary but is divided between pro-surveillance and pro-privacy groups.[8] The purposes for which surveillance technologies are used are numerous. Guzik argues that these technologies are not only used by state authorities to monitor individuals (as is the mainstream view), but also to monitor things that the individuals use,[9] that form part of the 'internet of things'.[10]

Privacy today, in the context of AI and other technologies, has undergone significant transformations compared to the understanding prevalent during the establishment of international frameworks such as the International Bill of Rights, the African Charter on Human and Peoples' Rights (African Charter) and the Cybercrime Convention.[11] The advancements in AI and technology have brought forth new challenges and complexities that have reshaped the landscape of privacy. With the proliferation of digital platforms, interconnected devices and data-driven algorithms, individuals' personal information is now more extensively collected, analysed and shared than ever before. The scale, speed and granularity of data collection have surpassed what was envisioned in earlier frameworks. Additionally, the opaque nature of AI algorithms and the widespread adoption of surveillance technologies have raised concerns regarding individual autonomy and the potential for discrimination and abuses of power.[12] Therefore, the understanding of privacy today encompasses not only

[4] K Guzik 'Surveillance technologies and states of security' in K Guzik (ed) *Making things stick: Surveillance technologies and Mexico's war on crime* (2016) 1.

[5] Feldstein (n 3).

[6] As above.

[7] B Kirstie & L Snider (eds) *The surveillance-industrial complex: A political economy of surveillance* (2019).

[8] HA Ünver *Politics of digital surveillance, national security and privacy* (2018).

[9] Guzik (n 4) 13.

[10] R van Kranenburg 'The internet of things: Radical transparency within the reach of all' (2011) 15 *Journal of International Issues* 126.

[11] 'Privacy and data protection', https://dig.watch/topics/privacy-and-data-protection (accessed 27 July 2023).

[12] M Rijmenam 'Privacy in the age of AI: Risks, challenges and solutions' (2023), https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/ (accessed 27 July 2023).

the traditional notions of personal space and confidentiality, but also the protection of individuals' digital identities, control over personal data, transparency in data processing, and safeguarding against potential algorithmic biases and privacy intrusions inherent in AI systems and other emerging technologies.[13]

AI surveillance technology comes with huge risks, which can be viewed from a variety of perspectives, such as economics and international affairs, as well as human rights. The former is concerned with the technology's monopolistic and centralising characteristics, owing to the massive scale required by both businesses and nations, as well as the potential risks of data colonialism.[14] On the other hand, the latter is concerned with the impact of AI surveillance on fundamental human rights. Owing to the negative implications of AI technology, surveillance practices by governments have faced criticism from activists and human rights organisations. These groups argue that such measures compromise individuals' right to privacy and freedom of expression. As such, they advocate transparent and accountable surveillance policies that respect citizens' civil liberties.[15] Additionally, the international community has occasionally raised concerns over potential abuses of surveillance technologies in Africa, necessitating a closer examination of their role in shaping policy and public opinion.[16]

To examine the extent of AI surveillance in Africa and its implications for human rights, this article first considers the prevailing situation in some countries in Africa as far as AI surveillance is concerned, so as to establish developments made in the uptake of AI. It then examines the general benefits of AI surveillance that Africa can leverage to its benefit and the concerns raised regarding the said developments. The article also assesses the effectiveness of the legal and institutional safeguards that various African states have put in place to guard against potential adverse effects of the technology. Lastly, the article concludes by highlighting areas for improvement, especially on the part of states to ensure that the adoption of AI technology is accompanied by the necessary regulatory protections to avert potential negative impacts on fundamental rights. Notably, while African states have adopted differing approaches in the uptake

[13] J Hoven *Privacy and information technology*'.

[14] U Sahbaz 'Artificial intelligence and the risk of new colonialism' (2019) 14 *Horizons: Journal of International Relations and Sustainable Development* 58.

[15] OHCHR 'Surveillance and human rights' (2019) Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression 3.

[16] B Jilli 'The spread of surveillance technology in Africa stirs security concerns' 11 December 2020, https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/ (accessed 27 July 2020).

of AI, this article seeks to report on trends observed in various parts in the region.

2 Situation in Africa

In Africa, AI is already being employed in diverse sectors such as health care, finance, manufacturing, transport, military technology and, now, surveillance technology. Authorities from all over the world utilise cutting-edge techniques to monitor populations in the name of safeguarding their security interests.[17] At least 14 states in Africa (Mauritius, South Africa, Zambia, Zimbabwe, Botswana, Nigeria, Rwanda, Kenya, Uganda, Egypt, Algeria, Namibia, Ghana and Côte d'Ivoire) have already begun using techniques such as smart policing and safe cities and, as a matter of course, the rest are likely to follow suit. This technology has been employed by these states for two major purposes, namely, to monitor their citizens through video surveillance and biometric tracking[18] and to control criminal behaviour. Elsewhere in the Global South, as it were, such as in Mexico, where monitoring, mobility, communication and identification are inherent to strategies of governance, surveillance has been embraced and employed to fight organised crime and has been shown not only to reduce insecurity but also to influence contemporary governance.[19] It is seen as both politically vital and popular in some parts in the Global North, where there has been an increased threat of terrorism, far-right radicalisation and extremist groups.[20] However, in an effort to strike a balance between surveillance and privacy rights, regions such as the European Union (EU) have begun to implement safeguards to prevent the misuse of public surveillance systems.[21]

Returning to Africa, the adoption of AI surveillance in the region has been aided by increased investments and infrastructure-building efforts by foreign governments in Asia and Europe. In recent years, Chinese companies, led by Huawei, the top supplier of sophisticated surveillance technologies, have not only been heavily involved in such operations but have also been identified as 'global leaders'. While pitching the safe city model to national security agencies, it is

[17] Guzik (n 4) 7.

[18] MS Cataleta *Humane artificial intelligence: The fragility of human rights facing AI* (2020).

[19] Guzik (n 4) 10.

[20] Ünver (n 8) 1.

[21] J Vincent 'EU draft legislation will ban AI for mass biometric surveillance and predictive policing' *The Verge* 2023, https://www.theverge.com/2023/5/11/23719694/eu-ai-act-draft-approved-prohibitions-surveillance-predictive-policing (accessed 27 July 2023).

reported to have introduced smart city technology in 90 countries (including 230 cities) and is currently helping the Saudi Arabian government build safe cities, and attempting to penetrate new sub-Saharan African markets.[22] It has been reported that public firms are collaborating with private firms to export authoritarian technologies to liberal democracies and authoritarian states with similar ideologies, in order to expand their influence and promote alternative forms of governance.[23] The importers of these technologies, who would otherwise have limited access to such technology, if at all, include Zimbabwe.[24]

The spread of AI surveillance technology is also evident in Ethiopia, Zambia and Uganda. In Ethiopia, concerns have been raised as the country has already begun importing the technology. Specifically, the country has attempted to expand its comparatively advanced information and communication technology (ICT) hub with Chinese support, whose involvement, although discounted by a subsequent study, is allegedly guided by political motives, among others, to diffuse surveillance capabilities.[25] This is particularly so because of Ethiopia's historically heavy surveillance and repressive practices.[26] In Uganda and Zambia, government officials have been revealed to have used AI surveillance technology with the help of Huawei technicians to spy on political opponents.[27] Their private communications were allegedly intercepted, and the information that was extracted was then utilised to impede and undermine genuine democratic action.[28] Even worse, Huawei staff members prompted security officials to travel to Algiers to examine Huawei's intelligence video surveillance system, which was followed by Uganda's purchase of a comparable facial recognition surveillance system from Huawei for US $126 million.[29] These instances contribute to the claim that the adoption of AI surveillance technology has not been accompanied by the necessary regulatory protections, with potentially negative impacts on fundamental rights. On the other hand, there is a dire need to

[22] Feldstein (n 3) 14.

[23] Feldstein (n 3) 13.

[24] Feldstein (n 3) 14.

[25] J Meester '"Designed in Ethiopia" and "Made in China": Sino-Ethiopian technology collaboration in south-south relations' CRU Policy Brief (2021).

[26] Meester (n 25) 1.

[27] J Parkison, N Bariyo & Chin 'Huawei technicians helped African governments spy on political opponents' 14 August 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 (accessed 10 November 2022).

[28] A Mavedzenge 'The right to privacy v national security in Africa: Towards a legislative framework which guarantees proportionality in communications surveillance' (2020) 12 *African Journal of Legal Studies* 360.

[29] E Biryabarema 'Uganda's cash strapped cops spend $126 million on CCTV from Huawei' *Reuters* 15 August 2019, https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF (accessed 10 November 2022).

avoid deluding and, therefore, entrapping oneself by adopting an alarmist response and stressing the risks. Instead, a more uplifting narrative should be adopted that emphasises positive outcomes for ICT cooperation with European states, especially in the absence of proof of the politicised narratives surrounding foreign involvement in Africa, after putting them to the test against real-world initiatives.[30] This notion is informed by the inherent merits of AI surveillance on crime prevention, emergency detection and general public safety. That said, the article will first turn to the benefits that AI surveillance technologies may present before looking at the concerns, the safeguards in place and their efficacy.

3 Benefits of AI surveillance in the African context

AI surveillance can help address challenges general to the world and specific to Africa. According to recent studies, surveillance is a common practice employed in many African states to obtain the data needed to deter criminal efforts or to uncover the identity of offenders.[31] It is crucial that governments ensure peace and security, especially in developing countries, which have likewise faced challenges such as insecurity, political instability, civil conflict, and related issues. In this regard, the benefits of AI surveillance in aiding criminal justice, particularly in reducing crimes such as terrorism and ensuring long-term security, cannot be overlooked.[32] Indeed, it is only within a safe and peaceful environment that developing economies in Africa can develop.[33]

Electronic surveillance and communication interception may also be necessary for the protection of fundamental human rights such as the right to privacy.[34] African states are also not necessarily fully compliant with their human rights obligations, as is demonstrated further in the part that examines the regional and international human rights frameworks. As such, surveillance to the extent necessary for the performance of legitimate obligations ought to be promoted and encouraged. Furthermore, AI can help in making better and fairer decisions, even though the resulting biases are profoundly

[30] Meester (n 25) 1.

[31] Mavedzenge (n 28).

[32] Cataleta (n 18).

[33] P Alston & M Robinson *Human rights and development: Towards mutual reinforcement* (2009).

[34] Mavedzenge (n 28).

limiting[35] which, after all, is not a reason to reject it entirely.[36] For instance, AI can assist in the criminal justice system by providing data-driven insights to aid in decision making, such as predicting recidivism rates or identifying patterns in crime data. This contributes to fair administrative action and in the long term advances good governance because as decision makers make decisions likely to adversely affect certain individuals and groups, they are intended to consider objective factors backed by evidence. As such, even though AI surveillance may have limitations, its benefits, viewed optimistically, outweigh the demerits if the concerns that arise are sufficiently addressed.

4 Challenges presented by AI surveillance in Africa

4.1 General data protection issues

Several academics have asserted that the use of digital technology, such as electronic mail, makes it nearly impossible to completely avoid being monitored.[37] The said surveillance has the potential to directly or indirectly affect human rights. For instance, unchecked AI surveillance poses a threat to fundamental democratic principles, including public participation.[38] Citizens may withhold their true opinions and adopt those that are politically correct for fear that their beliefs may be used against them in the future because they are indelibly surveilled. While not directly related to human rights, the effects on democracy are important to note. However, in examining challenges posed by general data protection issues, this part will address three general categories of concerns which include the procurement and/or deployment of the technology; the storage and processing of data; and the use of data.

The first concern relates to the transparency of procurement and/or deployment of the technology. AI surveillance technology is not necessarily being procured from the providers/developers or deployed in a transparent manner. In Ethiopia, China's influence on the country's surveillance practices touches upon crucial information

[35] J Hurwitz & M Peffley 'And justice for some: Race, crime, and punishment in the US criminal justice system' (2010) 43 *Canadian Journal of Political Science* 457.

[36] E Santow 'Can artificial intelligence be trusted with our human rights?' (2020) 91 *Australian Quarterly* 10.

[37] R Stallman 'What we need to learn from Snowden: Only by organising politically for human rights, including privacy rights, can we raise awareness of the dangers of Big Brother state surveillance' (2013) 48 *Economic and Political Weekly* 82.

[38] S Feldstein and others *The global struggle over AI surveillance: Emerging trends and democratic response*' (2022).

but is highly unlikely to be disclosed to the public. Notably, technology development and deployment are important aspects that have been neglected in the surveillance-privacy discourse. This issue presents an access to information concern. In terms of the transparency requirement, it is crucial for the people who are potential subjects of a certain technology to be made aware of the source, so as to enable them to conduct the necessary inquiry as to the motives of such acquisition. Considering the influence that AI technology providers have on the surveillance industrial complex, the introduction of AI surveillance technology should be accompanied by some form of regulations or checks and balances.

The second concern relates to the storage and processing and use of the data. According to research, analysis of data stored by state agencies 'may be both extremely revealing and intrusive, particularly when the data is merged and collated'.[39] The issue here is how state actors process, store and use the large amounts of data collected by AI surveillance technology. As per studies, communications data is 'storable, searchable, and accessible, and its release to and utilisation by state agencies is essentially unfettered'.[40] In practice, this is illustrated by Uganda's efforts to intercept opponents' communications to gain political advantage and even acquire expensive technology in what may be argued to be a similar context.

The third concern relates to the use of the data after relevant processing techniques have been employed. Data may be used to profile and discriminate against people in decision making, thereby violating the rights to equality and non-discrimination. This may be based on various factors previously identified during surveillance through their observable behaviour. Studies have shown that the use of monitoring as a method of organisational control can be used to bolster the interests and perspectives of some players while undermining or suppressing those of others.[41] Consequently, the use to which data obtained during surveillance is put is the ultimate determinant of whether the breach of privacy is justified and proportionate.

4.2 Human rights issues in particular

AI surveillance technologies have become pervasive in today's society, with both state and non-state actors participating in their

[39] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank la Rue, A/HRC/23/40 (2013).

[40] Feldstein and others (n 38); La Reu (n 39).

[41] Kirstie & Snider (n 7).

development, deployment and utilisation. While state actors have greater resources and legal authority, non-state actors, such as private companies and cybercriminals, also play a significant role.

4.2.1 State actors

The data protection issues discussed above raise a huge privacy concern, which merits serious attention and comprehensive consideration. This begs the question as to what the particular rights involved are. For starters, the rights encompass privacy and other civil liberties.[42] It has been demonstrated that surveillance affects not only privacy but also the rights that are shielded by privacy, including the ability to learn, create, talk, disagree, share ideas, and participate in politics without being paralyzed by the fear of government supervision and interference.[43] Furthermore, studies have demonstrated that AI-powered technology (such as surveillance) can result in the same human rights violations that it is intended to prevent.[44] One of these violations include algorithmic bias and discrimination. AI algorithms can inherit the biases present in the data they are trained on, hence leading to discriminatory outcomes. This bias can disproportionately impact certain groups based on race, ethnicity, gender or other characteristics.[45] Additionally, AI-generated evidence in legal proceedings can raise questions about the reliability and validity of the information presented.[46] Without proper safeguards and oversight, AI surveillance can undermine due process and fair trials. Lastly, AI-powered facial recognition at airports[47] and border crossings can raise concerns about the freedom of movement. The constant monitoring and profiling of travellers may lead to unnecessary suspicion and restricted travel for innocent individuals.

As for privacy, governments are allegedly conducting investigations in an unduly intrusive way that threatens people's right to privacy in order to combat terrorism, organised crime and other vices.[48] For

[42] I Gagliardone 'The impact of Chinese tech provision on civil liberties in Africa' (2020) 99 *SAIIA Policy Insights* 1.

[43] H Shamsi & A Abdo 'Privacy and surveillance post-9/11' (2011) 38 *Human Rights* 17.

[44] Santow (n 36).

[45] M James & S Jake 'What do we do about the biases in AI?' (2019) *Harvard Business Review* para 2.

[46] QT Katherine, V Plixavra & R Sofie 'Legal challenges in bringing AI evidence to the criminal courtroom' (2021) 12 *New Journal of European Criminal Law* 531.

[47] S Rebecca & G Rick 'TSA is testing facial recognition at more airports, raising privacy concerns' *Washington News* 15 May 2023.

[48] A Gwagwa & Others *Protecting the right to privacy in Africa in the digital age* (2014) 2.

the foregoing reasons, the procurement of sophisticated technology without following due process and its subsequent application in the collection of data constitutes a violation, or at least a limitation, of individual privacy. Further, when the data collected is used to profile individuals, it could result in future illegitimate and disproportionate discrimination on various bases observed during surveillance.[49] For instance, a data processor may be able to establish a data subject's marital status and draw adverse inferences from it, and subsequently utilise this information to inform crucial decisions such as whether to hire them. This turns into a human rights concern since unchecked state monitoring exposes a person to arbitrary or unlawful intrusion into their family, home or communications, breaching their right to privacy as well as other related rights, including the right to freedom of expression or freedom of association.[50]

Multiple other practical challenges are encountered in efforts to ensure a human rights-sensitive surveillance programme. For instance, Ünver[51] contends that two crucial parts of the surveillance-privacy controversy in the digital domain have been ignored, namely, the surveillance-industrial complex and the race for technological superiority.[52] The former drives a state's willingness to hoard secrets or to reveal certain key information in the interests of legitimacy, while the latter drives a state's willingness to disclose policy information as a result of rising costs of acquiring vital intelligence in an interconnected world. However, these problems, which were present in traditional surveillance methods, have since been overcome by AI surveillance and are therefore no longer a challenge in scale and duration. Costs of technology and data storage are declining, as well as reliance on security forces, thereby removing some of the financial and practical impediments to conducting surveillance, resulting in enhanced state capacity to conduct simultaneous, invasive, targeted and broad-scale surveillance.[53]

4.2.2 Non-state actors

Addressing the threats posed by non-state actors in AI surveillance requires a multifaceted approach, involving robust legal frameworks,

[49] Cataleta (n 18).
[50] Feldstein (n 3).
[51] Ünver (n 8).
[52] The connection between the massive multinational conglomerates that manufacture, distribute and promote technologies of surveillance, the institutions of social control and civil society has an influence on surveillance policy. See Kirstie & Snider (n 7).
[53] Feldstein & Others (n 38).

regulatory measures and public awareness.[54] It is crucial to strike a balance between technological advancements and protecting fundamental human rights. Private technology companies have increasingly embraced AI surveillance systems for various purposes, including facial recognition, behaviour tracking and data analysis.[55] While these technologies offer benefits such as enhanced security and efficient services, they raise concerns regarding human rights and privacy. The extensive collection of personal data without explicit consent, potential misuse or unauthorised access to sensitive information, and the perpetuation of discriminatory practices all jeopardise individuals' rights to privacy, autonomy and non-discrimination.[56] Moreover, the lack of transparency and accountability in private companies' surveillance practices exacerbates these concerns. Non-state actors operating outside of legal frameworks and regulatory oversight may exploit the collected data for commercial gains, compromise privacy, and contribute to a surveillance culture that erodes human rights.[57]

Non-state actors, including individual hackers and organised cybercriminal groups, pose additional threats to human rights in the context of AI surveillance. These actors exploit vulnerabilities in surveillance systems, manipulate data and breach security measures.[58] Their activities may lead to unauthorised surveillance, invasion of privacy, and even malicious manipulation of AI systems. By targeting individuals or organisations, hackers compromise the right to privacy, freedom of expression and freedom of association. Furthermore, the unauthorised access and manipulation of surveillance data can have severe implications for personal safety, reputation and overall trust in digital systems.[59] The power wielded by non-state actors in the realm of AI surveillance necessitates robust cybersecurity measures and legal protections to safeguard human rights.

In some instances, non-state actors, such as vigilante groups or activists, deploy AI surveillance technologies with the intention of

[54] European Parliament: 'European Union, 2020: The ethics of artificial intelligence: Issues and initiatives' (2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf (accessed 27 July 2023).

[55] Feldstein (n 3).

[56] Report of the OHRHR Annex 2 '*The human right to privacy: A gender perspective*' (2019).

[57] European Parliament (n 54).

[58] S Kreps 'Democratising harm: Artificial intelligence in the hands of nonstate actors', https://www.brookings.edu/wpcontent/uploads/2021/11/FP_20211122_ai_nonstate_actors_kreps.pdf (accessed 27 July 2023).

[59] L Tawalbeh '*IoT privacy and security: Challenges and solutions*' (2020), https://www.mdpi.com/2076-3417/10/12/4102 (accessed 27 July 2023).

exposing wrongdoing or promoting social justice.[60] While their motivations may be driven by legitimate concerns, the application of surveillance by non-state actors can still infringe upon individuals' rights to privacy and freedom of expression.[61] These groups might engage in vigilantism, engaging in surveillance activities without proper oversight or accountability. This can lead to the targeting and harassment of, or false accusations against innocent individuals, creating a climate of fear and inhibiting the exercise of fundamental human rights. Striking a balance between the pursuit of justice and the preservation of individual rights is crucial when non-state actors engage in AI surveillance for activism or vigilante purposes. All these factors go to demonstrate why AI surveillance poses a considerable threat to human rights, given the extent of both state and non-state actors' participation.

4.3 The complex landscape of regulatory models for AI tools

The rapid advancement of AI technologies has introduced a multitude of transformative possibilities across various industries and sectors. However, the unchecked growth of AI tools has raised concerns about potential risks and ethical implications. To address these issues, effective regulation is necessary, considering the lack of a unitary definition for AI, its contextual usage and its impact on diverse legal domains.[62] The absence of a unified characterisation for AI[63] presents formidable hurdles in formulating regulatory frameworks for AI tools. This predicament arises due to the diverse nature of AI, encompassing a wide array of technologies and applications. The lack of a universally embraced definition for AI engenders several challenges.[64] For example, it may lead to ambiguity and inconsistency. Distinct stakeholders, including researchers, policy makers and industry experts, may hold disparate interpretations of AI. Consequently, regulatory frameworks developed by various authorities may diverge in scope and depth, leading to incongruities in the assessment and governance of AI tools across different jurisdictions. Furthermore,

[60] NT Lee 'Police surveillance and facial recognition: Why data privacy is imperative for communities of colour' *(*2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ (accessed 27 July 2023).

[61] P Albrecht and others (eds) *Perspectives on involving non-state and customary actors in justice and security reform* (2011).

[62] C Novelli and others 'Accountability in artificial intelligence: What it is and how it works' (2023), https://link.springer.com/article/10.1007/s00146-023-01635-y (accessed 27 July 2023).

[63] M O'Shaughnessy 'One of the biggest problems in regulating AI is agreeing on a definition' (2022), https://carnegieendowment.org/posts/2022/10/one-of-the-biggest-problems-in-regulating-ai-is-agreeing-on-a-definition?lang=en (accessed 27 July 2023).

[64] As above.

the absence of a well-defined characterisation for AI can hinder endeavours to address ethical and societal concerns pertaining to its deployment. Issues such as algorithmic bias that may lead to gender bias,[65] privacy infringements, and the impact of AI on jobs and human autonomy necessitate thoughtful regulation. Without a standardised definition, formulating ethical guidelines that apply universally to AI systems becomes a challenging task.

Contextual usage also impacts the potential risks associated with AI, making a one-size-fits-all regulatory approach impractical.[66] The same AI technology might be utilised in health care, finance, transportation and other domains, each requiring tailored regulations to address sector-specific concerns.[67] Similarly, AI's far-reaching implications transcend legal boundaries, affecting intellectual property rights, privacy, liability, and more. This creates a complex interplay between different legal domains and necessitates an integrated approach to regulation. Failure to address these issues comprehensively may result in regulatory gaps and inadequate protection for individuals and businesses.

5 Efficacy of human rights law in regulating AI surveillance technology

5.1 General international standards

Efforts to regulate and safeguard surveillance mechanisms have been ineffective due to the dynamism of surveillance in terms of methods and technologies as well as circumvention techniques.[68] Here, people may circumvent surveillance regulations so as to protect their privacy, avoid government censorship or engage in illegal activities. To understand the approach to safeguarding human rights, one must first appreciate this reality and, second, the nature of the rights subject to protection as well as the nature of state obligations. A common characteristic of civil and political rights, such as the right to privacy for present purposes (very generally), is that they guarantee non-action by state authorities with respect to citizens' activities (freedom from intervention).[69] As such, they may appear

[65] UNESCO *Artificial intelligence: Examples of ethical dilemma*' (2023).

[66] Novelli and others (n 62).

[67] D West & J Allen 'How artificial intelligence is transforming the world' (2018), https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/ (accessed 27 July 2023).

[68] Ünver (n 8).

[69] N Ando 'National implementation and interpretation' in D Shelton (ed) *Oxford handbook of international human rights law* (2013) 717.

to be the easiest to implement. This is inaccurate, though, as states must adopt a variety of measures to ensure that their commitments regarding this class of rights are upheld, such as allocating funds for the fulfillment of civil and political rights.

In an effort to control communications surveillance, the international community has created a set of rules and norms.[70] Arguably the most crucial among these is the principle of proportionality to which state parties to the International Covenant on Civil and Political Rights (ICCPR) must adhere, as it is expressly provided for.[71] According to the principle, states have a responsibility to ensure that any such invasion of privacy is reasonable given the aim desired and that communication surveillance must be carried out in line with the law and in a proportionate manner where it is necessary.[72] An ideal proportionality analysis is comprehensive and comprises three main tests, preceded by two preliminary tests – the legality test and the legitimate aim test. The former assesses whether the interference has a basis in national law, whereas the latter evaluates whether the impugned measure is pursuant to or in consonance with a particular legitimate aim.[73] When using the proportionality principle, three additional checks follow, the first two dealing with efficiency and the last with an empirical evaluation of the relative weights and trade-offs of competing values. The three main tests are the necessity or less restrictive alternative or minimal impairment test, which examines whether the measure chosen was the one least restricting the rights in question; the suitability or rationality test, which examines whether a measure that interferes with an individual's right is suitable for achieving the legitimate aim; and the strict proportionality test, which examines whether the harm to the person is excessive as compared to the benefits to be obtained.[74]

Specifically, international human rights law has established guiding principles for determining whether a given monitoring operation is legal at whatever stage it is conducted, that is, collection, storage and use. These principles utilise a tripartite test comprising a domestic legal framework allowing for surveillance, necessity and proportionality of surveillance, and a legitimate justification. First,[75]

[70] International Principles on the Application of Human Rights to Communications Surveillance (2013).

[71] Art 17 International Covenant on Civil and Political Rights.

[72] *MG v Germany* Communication 1482/2006 paras 10.1 and 10.2.

[73] Y Arai-Takahashi 'Proportionality' in Shelton (n 69) 451.

[74] As above.

[75] Surveillance and human rights. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/41/35 (2019).

the legal system must be open to the public, transparent, clear, all-inclusive and non-discriminatory. Regulatory provisions ought to be written in sufficient detail to allow people to govern their operations as needed.[76] The second criterion is that surveillance must only be used when it is absolutely and clearly essential to accomplish a lawful goal (the international legal standard of necessity and proportionality).[77] Third, monitoring is only acceptable when it serves the interests of the entire country.[78] Even the justifications for monitoring, such as maintaining public order and protecting national security, should not serve as an excuse for arbitrary or unreasonable restrictions on individual rights to free speech. In this regard, states have the obligation to do three things. They must first prove that a particular expression endangers a clear interest in public order or national security. Second, they must undertake action to ensure the presence of a robust, independent oversight system. Third, they need a judiciary that approves pertinent surveillance techniques and offers redress when abuse occurs. The creation of a legal framework that ensures proportionality in communications interception is recommended in this regard.[79] A legislative and institutional framework must be followed with implementation, particularly at a national level. National implementation of human rights law using various mechanisms entails an elaborate, difficult and time-consuming but inescapable and necessary endeavour that requires practical balancing of reality with ideals, if a meaningful outcome is to be attained.[80] The next part interrogates the extent to which African states have achieved these ambitious international standards meant to safeguard fundamental human rights that may potentially be violated in the course of otherwise beneficial AI surveillance.

Ideally, state parties to the relevant conventions are bound to comply with these standards to legitimately carry out surveillance. The problem, however, is that the demands are too high, and governments do not meet them. The lack of proper national law and enforcement mechanisms, lax procedural safeguards and ineffective oversight systems have generally been cited as causes of states' fairly low accountability. Surprisingly, even democracies with a history of upholding the rule of law and strong monitoring structures

[76] Rather than vague or overbroad, essentially allowing unconstrained discretion to government officials.

[77] Proportionality has been argued to not only be a morally relevant criterion by which to assess surveillance, but also a necessary criterion. See K Macnish 'An eye for an eye: Proportionality and surveillance' (2015) 18 *Ethical Theory and Moral Practice* 529.

[78] Excluding surveillance conducted in the sole interest of a government, regime or power group, see Feldstein & Others (n 33).

[79] Mavedzenge (n 28).

[80] Ando (n 69) 717.

regularly fall short in their efforts to appropriately protect individual rights when implementing surveillance programmes.[81] Accordingly, this article assesses whether African governments have violated surveillance laws, lacked judicial oversight of surveillance powers, and been secretive in a way that has eroded checks and balances.

5.2 African landscape and practice

Although the challenges discussed above are manifest in the case of Africa, it would be incorrect to suggest that nothing has been done. All African states except Morocco are state parties to the African Charter. The Charter, however, is silent on the right to privacy and fails to recognise it expressly in its text. This conspicuous omission of an important right entrenched in all other human rights instruments has been highlighted by scholars as a huge limitation. This is especially so because the rationale for removal of the provisions from the initial drafts of the African Charter at the negotiation stages was informed by, as it were, African communitarian values, which arguably have manifested in the non-observance of the tenets that the right connotes, as it is, constantly infringed in many jurisdictions in Africa.[82] It has been suggested that such rights that have been omitted can be incorporated by three alternative ways, namely, the adoption of protocols to the African Charter,[83] the thoughtful and forward-thinking application of the rules in line with international norms and standards[84] or the amendment of the Charter by states as they deem appropriate.[85]

Unfortunately, African states have performed poorly in fulfilling their obligations and have failed to even fulfil their reporting obligations.[86] As such, the gap between international and municipal law enforcement continues to widen as new norms and practices are codified at the international level, then ignored or codified and not enforced at the national level, demonstrating the disconnect between codified 'minimum' international human rights standards with the municipal legal system.[87]

[81] Mavedzenge (n 28).

[82] M Mbondenyi *International human rights and their enforcement in Africa* (2011) 397.

[83] CH Heyns 'The African regional human rights system: In need of reform?' (2010) 10 *African Human Rights Law Journal* 173.

[84] R Murray 'Report on the 1996 sessions of the African Commission on Human and Peoples' Rights 19th and 20th sessions' (1997) 18 *Human Rights Law Journal* 923.

[85] Mbondenyi (n 60) 403.

[86] ICJ Kenya & ICJ-Sweden *Human rights litigation and the domestication of human rights standards in sub-Saharan Africa* (2007).

[87] As above.

That notwithstanding, almost 50 per cent of African states have given recognition to the right to privacy in their constitutions.[88] The fundamental rights explicitly listed in the African Charter may be used to infer state obligations to respect and safeguard specific rights aspects.[89] The fact that at least 13 African states have passed laws enabling the government to undertake electronic surveillance and intercept private conversations serves as an illustration of this. In any event, the African Union (AU) Convention on Cyber Security and Personal Data Protection, adopted in 2014, governs four key areas, including electronic transactions, personal data protection, cyber security and cybercrime, and establishes a legal framework for cyber security and data protection. These actions cumulatively reaffirm their commitment to fundamental freedoms and human rights contained in instruments adopted in the regional and international frameworks. However, it has been criticised for containing ambiguous terms that give broad room for interpretation[90] and failing to specify clear minimum thresholds, allowing leeway for governments to avoid implementing substantial regulation.[91]

Whether or not these duties are legally obligatory, they are likely to be ignored by African nations that lack effective legal enforcement or those with authoritarian systems. As a result, AI surveillance technology may end up being procured, stored on devices, processed, and subsequently used without legal and/or institutional checks and balances, thereby resulting in human rights violations. This occurrence, which should be averted, is well articulated by Shamsi and Abdo who, albeit in a different context, assessed the impact of surveillance on privacy rights in the United States (US) post 9/11.[92] In essence, the US administration's post-September 11 surveillance policy failed to distinguish between surveillance for law enforcement and intelligence-collecting purposes. The surveillance programmes instituted in the aftermath of the terror attack have typically functioned 'beyond the rule of law, subject solely to restrictions and political expedience, rather than within it, subject to judicial review and political responsibility'. Shamsi and Abdo maintain that this constitutes a structural failure of the nation's systems of checks and balances (that is, the system of intertwined oversight in which the power of one branch of government in respect

[88] Mavedzenge (n 28) 2.

[89] As above.

[90] P Ugwu 'Analyst picks holes in proposed AU Cybersecurity Convention' (2014), http://nigeriacommunicationsweek.com.ng/e-business/analyst-picks-holes-in-proposed-au-cybersecurity-convention (accessed 10 November 2022).

[91] http://www.thezimbabwean.co/news/zimbabwe/72617/the-african-union-convention-on.html (accessed 10 November 2022).

[92] Shamsi & Abdo (n 43).

of constitutional decision making is constrained by the oversight of the others) to keep pace with the rapid technological revolution, thereby essentially permitting mass government surveillance and data mining. Regarding the effects on human rights, they believe that it has resulted in the deterioration of privacy rights. According to them, the issue is not the legislation itself but rather the fact that the executive branch frequently violates it, the legislative branch does little to stop these violations or even sanction them, and the court arbitrarily rejects serious objections to surveillance on technical grounds.[93]

As a result, the legally sanctioned procedure for obtaining permission to conduct surveillance must include adequate checks and balances to provide a proportional balance between preserving privacy and safeguarding national security, by ensuring that privacy is not unduly restricted.[94] The necessity that permission for surveillance be granted by a qualified, unbiased and autonomous authority is one check and balance method.[95] Literature reveals that three major approaches have been taken by African states in respect of authorisations for communications surveillance, namely, the executive approach, the judicial approach and a hybrid of the two, each presenting its peculiar challenges.[96] As the wording suggests, the first involves a member of the executive, the second involves a court, and the third involves a mixture of both. All are equally effective provided they include sufficient safeguards to ensure respect for data protection principles. However, it has been noted that the necessary objective and unbiased examination can only be performed by a body that is objective, self-sufficient and technologically proficient in the area.[97] This is the crucial factor, and in order to take it into account, a four-part test must be applied to the decision-making authorities. The authority performing the communications surveillance must first be kept apart from it. It must be knowledgeable about these matters. It must also have the resources to carry out the tasks allocated to it. Finally, it must be qualified to decide on the legality of the tasks.

[93] As above.

[94] Mavedzenge (n 28).

[95] African Commission on Human and Peoples' Rights Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa (2015) 36.

[96] Mavedzenge (n 28).

[97] As above.

6 Way forward

European countries have been confronted with challenges,[98] mainly on making surveillance oversight transparent.[99] While their approaches and others[100] may not be necessarily suitable for replication in Africa, they may provide insight as to best practices employed to comply with international standards. Ünver recommends that democracies ought to improve their technological proficiency for oversight and, while undertaking the rather onerous task of oversight,[101] achieve a balance between privacy and monitoring that respects both human rights and the political culture of the nation.[102] In addition, scholars have urged stakeholders to ensure sufficient accountability in defending human rights as we give machines more responsibility for autonomous decision making.[103] In order to achieve this ambitious goal, which even advanced democracies have been unable to guarantee to a comprehensive extent, African states may consider several practices that have proved effective elsewhere, among others that have been discussed below. States are encouraged to carefully consider these practices as they scale up their efforts to ensure that human rights are safeguarded when using AI surveillance. As Mavedzenge observes, a principled rather than a formalistic approach would be most effective.[104]

First and foremost, even though new law is not necessarily the ideal solution, new regulation, particularly hard law which is best for reasons of enforcement, is necessary to supplement the existing legal framework.[105] Stallman proposes stringent measures such as restricting data collection, especially by the state, by designing systems that log activities not to keep personal identifying data for a very long time, in addition to legally restricting access to the accumulated data, which is the default action taken by campaigners and which by itself is insufficient as it may prevent decision makers from accessing important information and insights. To achieve this, he recommends collective action, rather than individual action, as the latter is less injurious.[106] Several challenges which are key

[98] Such as technological backwardness of safeguard and oversight mechanisms rendering them incapable of keeping up with technologically proficient intelligence agencies and citizen-driven circumvention tools; see Ünver (n 8).

[99] Ünver (n 8).

[100] C Arun 'Paper-thin safeguards and mass surveillance in India' (2014) 26 *National Law School of India Review* 105; S Mahapatra 'Digital surveillance and the threat to civil liberties in India' GIGA Focus (May 2021).

[101] Over the executive and intelligence community to detect abuse and excesses.

[102] Ünver (n 8) 1.

[103] Cataleta (n 18).

[104] Mavedzenge (n 28).

[105] Cataleta (n 18).

[106] Stallman (n 37).

considerations[107] present themselves, most notably that of rapid speed of technological development in relation to slow speed of legal enactment. In other words, new regulations are implemented far more slowly as compared to the velocity of technological progress.[108] The applicable national law with respect to technological progress may also be outdated, inadequate and unsuitable given its time of enactment and, therefore, not comprehensively covering unanticipated technological developments. Considering this, self-regulation and soft regulation can provide alternative models of regulation in the intervening period which serves to fill the gap pending enactment, which can later morph into hard law.

Second, the institutional framework needs to be more robust. Where a state's surveillance law is progressive and at par with the technological development in question, the state must then oversee its implementation through a well-formulated institutional framework at the national level. It may also leverage international institutions such as the UN human rights systems which has been recommended as a way of ensuring the transparency and accountability of data management (done by data holders such as states).[109]

Third, monitoring and openness must be provided by the legislation and institutions. A system of checks and balances cannot operate without meaningful accountability and transparency. Three components are required of the legislature. To ensure that privacy rights are safeguarded, the law governing surveillance should first be updated and modified. It should then strengthen the legal provisions that forbid the government from gathering information without a warrant and with reasonable grounds and, further, exert meaningful control over the executive to ensure that it adheres to the law.[110] The executive, in turn, must prohibit intelligence agencies from collecting data without proper procedures, restrict and regulate all intelligence activities, and publicly disclose any asserted legal authority for intercepting communications, along with the national legal justification for such actions.[111] The judiciary must also assume a more direct role in overseeing government surveillance and avoid theories of standing that effectively immunise executive action (in this case surveillance) from judicial review.[112]

[107] Cataleta (n 18).

[108] A Mantelero 'Come regolementare l'intelligenza artificiale: le vie possibili' (2019), https://www.agendadigitale.eu/cultura-digitale/come-regolamentare-lintelligenza-artificiale-ecco-i-temi-chiave/; ICJ Kenya & ICJ-Sweden (n 86).

[109] Office of the United Nations High Commissioner for Human Rights (OHCHR) *Guiding principles on business and human rights* (2011).

[110] Shamsi & Abdo (n 43) 9.

[111] Shamsi & Abdo (n 43) 17.

[112] As above.

Fourth, there is need to go further[113] to ensure the accountability of technology developers and evaluators (the conglomerates) from whom the states acquire the AI surveillance technology. This is particularly true because, even if a court may exercise oversight based on existing law, technology changes at a rapid rate and, as a result, laws can quickly become obsolete, as was the case in Algeria.[114] Regulating developers may require new regulations as the existing guides[115] are non-binding and violations may go unsanctioned.[116] In terms of self-regulation, creators must acknowledge the limitations of AI, particularly its potential to be exploited in ways that could violate human rights, and create surveillance systems (and, of course, regulations thereon) that capitalise on the contrasting strengths of humans and machines. There ought to be a global multisectoral governance structure that is based on rights and is geographically equitable that establishes pertinent standards to encourage accountability for technology developers, who would then be encouraged by governments to control the availability of developed products on the market and by external evaluators to ensure that their products satisfy human rights standards.[117]

Fifth, individuals and state actors should be more vigilant. They ought to be skeptical about AI surveillance in order to adopt the technology mindfully, thereby avoiding unnecessary harm. They must endeavour to interrogate the circumstances in which surveillance technology is obtained, the intention of so doing and its legitimacy, and whether, following installation, it is exploited for that particular purpose and in accordance with legal safeguards.

Sixth, in addition to state actors, non-state actors have a significant impact on the advancement of AI surveillance and therefore must be involved for optimal buy-in, given the significant impact local political economies have on the allocation and use of global capital and military engagements that make up surveillance systems.[118]

Lastly, the challenges posed by regulatory models for AI tools, including the absence of a unitary definition, contextual usage, and their impact on various legal domains, make crafting a robust regulatory framework a daunting task. While the holistic, sector-

[113] A Venkatasubramanian 'The human rights challenges of digital COVID-19 surveillance' (2020) 22 *Health and Human Rights* 79.

[114] Access Now 'COVID-19 contact tracing tools in MENA' 18 June 2020, https://www.accessnow.org/covid-19-contact-tracing-apps-in-mena-a-privacy-nightmare (accessed 10 November 2022).

[115] OHCHR (n 87).

[116] Venkatasubramanian (n 113) 82.

[117] As above.

[118] Kirstie & Snider (n 7).

specific, top-down and bottom-up approaches each have their merits and drawbacks, none can serve as a one-size-fits-all solution.[119] Instead, it is crucial to strike a balance by combining elements of different regulatory approaches while ensuring active involvement from all stakeholders. By fostering interdisciplinary collaboration, transparency and ongoing adaptation, we can create an AI regulatory framework that promotes innovation, protects individual rights, and addresses the evolving challenges of this transformative technology.

7 Conclusion

Africa has made significant, even commendable progress in embracing developments in technology, including surveillance technology, albeit with the rather peculiar assistance of states and corporations appearing to have vested interests and, therefore, pushing for the adoption of such. While this is beneficial in multiple ways and may be employed to address certain challenges specific to African countries, it presents serious challenges which, if not addressed, would have far-reaching negative implications for fundamental human rights. Although some progress has been achieved in terms of general human rights safeguards, African states are not adequately prepared or taking the requisite effort to be prepared to address, mitigate or entirely thwart unintended consequences of AI surveillance, at least to the set international standards. Consequently, the rate at which surveillance technology is proliferating in African states and the manner in which it is being adopted exposes Africans to possible violations of privacy and associated human rights. The adoption of this revolutionary technology has not been accompanied by the necessary regulatory protections. In particular, the existing law at an international, regional and national level, though binding, is either too generic or outdated or both. Compounded with inadequate procedural safeguards and institutional checks and balances, African states are left without safeguards to guard against the potential adverse implications of AI surveillance.

This article generally examines the extent of AI surveillance in Africa, its potential to become pervasive in the region, concerns and challenges that arise as a result, as well as the effectiveness of the prevailing legal and institutional frameworks to protect against human rights violations. It arrives at the conclusion that the adoption of this revolutionary technology has not been accompanied by the

[119] Simplilearn 'Top down approach vs bottom up approach: Understanding the differences' 17 February 2023, https://www.simplilearn.com/top-down-approach-vs-bottom-up-approach-article (accessed 27 July 2023).

necessary regulatory protections. Consequently, and in the absence of active efforts to remedy this situation, millions of Africans are still at risk of having their human rights violated, particularly their rights to privacy, with potentially negative impacts on other fundamental rights. In addition, the use of AI-based surveillance technologies in Africa raises serious concerns about the potential for bias and discrimination, as well as for inaccurate or unfair predictions about individuals. It therefore calls on states to scale up their efforts to ensure that human rights are safeguarded when using AI surveillance by implementing some if not all of the recommendations proposed.