Scope
Volume 16 Number 01 March 2026

Governing Artificial Intelligence for Peace and Security: A Comparative Europe–Africa Framework

Akinwale Victor, Ishola [1]; Anya Adebayo, Anya [2]; Kelechi Adura, Anya [3]; Eke Kehinde Anya [4]

[1]Department of Peace, Security and Humanitarian Studies, University of Ibadan
[2]Department of Political Science, Obafemi Awolowo University Ile-Ife
[3]Computer science, Landmark University Omu-Aran Nigeria
[4]Scottish Power Headquarters, Glasgow

Abstract: The fast incorporation of artificial intelligence (AI) in the structure of peace and security has revolutionized the modern trends in surveillance, policing, and conflict prevention. However, the control of AI in these areas is skewed and heavily influenced by institutional and capacity, regulatory customs and world power structures. This paper explores the regulation of AI in the context of peace and security using a comparative Europe Africa model, with references to empirical examples of facial recognition applications in criminal justice and the use of AI-assisted early warning mechanisms in conflict prevention. In reviewing the regulatory trends in the European Union and the new practices in African settings, the study questions the impacts of disparities in legal frameworks, data management, and organizational alignment on the implementation and management of high-risk applications of AI. Findings unveiled that not only the sophistication of technology influence the results of governance but also the regulatory capacity, organizational structure of data ownership, and engagement in international norm-setting processes. Although European models demonstrate the limiting nature of rights-based legal systems and institutional controls, most of the African situations deal with structural factors, such as inadequately integrated regulatory regimes and technical reliance on foreign powers. These inequalities demonstrate more general imbalances in how AI is governed by the global community and has consequences to civil liberties, responsibility and sustainable peacebuilding processes. This paper contends that to have effective AI governance of peace and security, there should be context sensitive and cooperative approaches that are not based on regulatory transplantation.
Wordcount: 251

Keywords: Artificial Intelligence, Peace & Security

Introduction

Artificial intelligence has rapidly become a significant tool in the modern peace and security architectures, transforming the way states and regional organisations can foresee conflict, monitor, regulate borders, and intervene in security situations. Although the policy and popular debates tend to denote AI as a technical innovation that can improve efficiency and accuracy in predictions, its increasing use in security governance prompts the discovery of a more profound list of political, ethical, and institutional issues. AI systems are integrated into existing power structures, legal orders, and security cultures, and their impacts on the results of peace and security are thus not neutral and uniform. In this regard, the main issue that AI presents in this area is not an issue of technological capacity, but a governance issue, namely, who creates, regulates, controls, and is answerable to AI-driven security procedures.

Governance challenges gain special importance when considered on a Europe-Africa dimension. Europe has a leading role in the global AI norm-setting, having comparatively sophisticated regulatory frameworks, institutional oversight structures, and a firm focus on human rights and rule-of-law values. Such circumstances have allowed European actors to treat AI governance as a regulatory issue that can be addressed using formal legal tools and institutional enforcement. Conversely, numerous states in Africa interact with AI in the pursuit of peace and security under far different structural conditions, which are characterised by asymmetrical regulatory capacity, limited resources, weak security contexts, and a high level of dependency on the technologies created externally. This is not a technical but a more political asymmetry that shows larger world hierarchies in knowledge production, regulatory power, and technological possession. The comparison between Europe and Africa should therefore not be perceived as a comparison between progress and lag, but as an exploration of the role of power, institutional capacity, and historical context in governing AI in a security context.

It is against this background that this paper analyses the regulation of artificial intelligence in the context of peace and security within Europe and Africa with specific reference to the institutional, regulatory, and political environment in which it is regulated.The study attempts to challenge the universalism of the current regulatory paradigms on the basis of exploring to what degree governance systems designed in European contexts can be sensitive to, or applicable in the African contexts of most security realities and institutional capacities. This emphasis is indicative of a larger issue in the global discourse of AI governance of the unequal distribution of regulatory powers, technologies, and ability to implement them to different regions.

Governing AI for Peace and Security: Comparative Contexts and Empirical Instances

Governance of artificial intelligence in surveillance and policing situations demonstrates one of the most acute conflicts between the security needs and the safeguarding of civil liberties. As an illustration of the most popular biometric AI application, facial recognition technology (FRT) demonstrates how similar technologies can have different governance effects in Europe and Africa, dependent on the law, institutional, and regulatory capacity, and enforcement. The legal and normative questions surrounding FRT have been characterized by continuing legal and normative challenge in Europe. Being a type of biometric data processing, FRT involves increased safeguards under the European law on data protection and privacy, and poses complicated legal challenges about the matters of proportionality, necessity, and basic rights (Canova and Simmler, 2024). These issues have been then converted into practical regulatory measures, both locally and supranationally. Some cities in Europe, such as Paris, have issued bans or limited use of FRT in the street, as concerns about mass surveillance are increasing and their effects on civil liberties are being questioned. The discussion around the proposed AI Act at the European Union level also highlights the challenge of balancing law enforcement goals and rights-focused governance. Despite the fact that AI Act seeks to normalize high-risk systems of the biometric, researchers have also highlighted the fact that legal authority of the FRT use by law enforcement agencies is not quite clear and comprehensive enough, thus providing ongoing legal loopholes (Canova & Simmler, 2024). European empirical case studies indicate that FRT can serve the purpose of public safety, but its implementation is linked to serious risks, such as discriminatory results and violations of civil rights, especially in cases where the checks and balances are not well established or defined (Lynch, 2024). The latter risks have led to the demand to strengthen regulation, including the suggestion of an overall prohibition on the use of FRT in the public, until effective accountability and oversight systems are established (Kuhlmann, 2024). The need to regulate biometric surveillance practices in a way that is principled, consistent with the rule of law, democratic accountability, and other established human rights principles has been highlighted by human rights advocates (Qandeel, 2024). Conversely, application of AI based biometric and surveillance systems in a number of African countries has taken place in vastly different governance contexts. The use of digital surveillance systems, like biometric identification systems and communication interception technologies, are growing across countries like Kenya, Nigeria, and Uganda commonly in conjunction with external technology providers. These technologies have increased the surveillance capabilities of the states, but their use has significantly surpassed the establishment of detailed legal and regulatory systems. Governments in Africa are projected to spend more than one billion dollars a year on digital surveillance systems, which is an indication of the

rising centrality of AI-enabled systems in national security strategies (Roberts et al., 2023). Yet, such expansion has often been achieved without robust data protection, transparency, and judicial controls. The existing empirical studies suggest that these deployments have facilitated large-scale types of mass surveillance that allow states to track the communication, movements, and identities of citizens with little to no responsibility (Roberts et al., 2023; Czuba, 2025). Civil rights violations and the abuse of gathered information have been worsened due to the absence of strong regulatory frameworks that govern surveillance technologies (Jili, 2022). The lack or inadequate data privacy regulations in places like Kenya has exposed citizens especially to the misuse of surveillance instruments even after it had been used pursuant to the intended purpose of security (Ischak, 2022). In contrast to Europe, where legal contestation and regulatory debate position the space of operation of FRT, the space of surveillance practices is in most instances not subject to any institutional constraining mechanisms in Africa. These empirical examples indicate that the peace and security implications of AI-enabled surveillance are influenced not by technology, but by governance. Although European encounters show that regulatory institutions can challenge, restrict, and re-calibrate the application of FRT, the African examples depict how the lack of regulations and external reliance on technology might strengthen the threats to civil liberties.

AI in Conflict Prevention and Early Warning

Artificial intelligence in conflict prevention and early warning has emerged as a more visible aspect of modern-day peace and security governance. With the ability to process large and multifaceted datasets, AI-powered systems have turned the conventional early warning systems (which are mostly descriptive) into predictive and anticipatory ones. These technologies are being implemented by both the European and African peace and security architectures to aid situational awareness, effective decision-making and preventive response. There is, however, more uneven governance and effectiveness of AI-enabled early warning systems that are influenced by institutional capacity, data availability and political coordination.

Early warning and conflict monitoring has long been a component of external action and peace missions within the European Union, with the Conflict Early Warning System (CFEWS) being one of the main data-centric analysis mechanisms. Emerging technological breakthroughs such as artificial intelligence and big data analytics have expanded the capabilities of the system to identify the patterns of conflict escalation and predict possible crises. The analysis of large volumes of data, detection of new risk factors, and a more accurate visualisation of the time and location of conflicts are practised with the help of AI technologies that will assist in responding to a more timely and precise intervention (Mandokhail, 2024; Selamet et al., 2025). The analytical functions of early

warning systems have been extended further by technological tools, including machine learning and natural language processing, which allow analyzing textual and digital sources, including media coverage and online discussion, in real-time (Muggah & Whitlock, 2022).

In addition to prediction, AI-based analytics have enhanced the use of data-driven decisions in European peace missions. These systems can process a large amount of complex data in seconds to provide a deeper understanding of the dynamics of conflict, highlighting the most important actors, and showing trends of interaction that can indicate an increased risk (Mandokhail, 2024; Selamet et al., 2025). In reality, AI has been applied to digital mediation situations, satellite-ceasefire tracking, and sentiment analysis of social media to generate a map of the popular opinion and online polarization. These applications facilitate near real-time peace operations, improving crisis mapping, early warning, and forecasting, and also help to develop strategies in view to effective mitigation of the conflict-related online dynamics (Zelizer et al., 2025). However, these AI-enabled systems have limitations on their effectiveness due to non-technical issues, such as deficiencies in political will, incomplete data, and coordination among stakeholders working on the conflict management (Ishola et al., 2025).Artificial intelligence in African peace and security, too, has a considerable potential in enhancing conflict prevention and early warning, especially in regional arrangements, e.g., the Economic Community of West African States (ECOWAS) and the African Union. The AI-based analytics can be used to help identify early warning signs by processing vast amounts of data and identifying patterns that would signal the development of a conflict or its escalation, thus allowing more proactive response to crisis management (Osee, 2024). The Continental Early Warning System (CEWS) within the African Union is one of the institutional platforms through which conflicts can be monitored and analysed in the continent. Although CEWS has achieved significant progress in the institutionalisation of early warning, its performance is constrained by human resource shortages, coordination and inconsistent integration of regional mechanisms (Noyes and Yarwood, 2013).

There are also structural and infrastructural barriers to the application of AI-based early warning systems in African contexts. The inability to access credible data, underdeveloped digital infrastructure, and the differences in technical capacity are one of the primary barriers to successful AI technologies implementation (Jegede and Ayuba, 2025). Besides, the aspect of utilizing external partners with regard to technical expertise and system development leads to the challenge of the local ownership, sustainability, and long-term institutional learning. This dependence can limit the capability of regional and national institutions to modify AI tools to localized security interactions and can solidify current imbalances in the generation of knowledge and technology worldwide (Souare, 2007).The experiences of the two regions, Europe and Africa reveal that although AI can greatly

improve conflict prevention and early warnings, it can only be effective under conditions of governance that goes beyond the technological advancement. The institutional capacity, data governance, political coordination, and ownership systems are critical determinants of the outcomes.

Key Governance Gaps and Power Asymmetries

The relative analysis of AI implementation in surveillance, policing, and conflict early warning in Europe and Africa indicates that the political issues related to artificial intelligence are not of technological nature, but institutional and political. The empirical instances presented in the previous sections indicate how differences in regulatory capability, data governance, and norm-setting capability influence the situation in which AI systems are developed, deployed, and challenged in peace and security. These inequalities create different forms of governance gaps and support prevailing power disparities between Europe and Africa. Major gap in governance relates to disparities in capacity to regulate. Characteristic of the context of Europe are comparatively strong legal systems, institutional systems of oversight, and means of judicial and civil challenge, all of which limit the application of AI applications with high risk in security affairs. The capability of European institutions to question, restrict, and rebalance the implementation of facial recognition technologies, and the current discussion of the EU AI Act, demonstrates how the European institutions can respond to the issue of the civil liberties concern. In comparison, the regulatory frameworks of the AI-enabled surveillance and early warning in many African states are disjointed, poorly developed, or inadequately implemented. The lack of detailed data protection regimes, scarcity of institutional control, and the capacity of the security agencies makes states less capable of controlling the use of AI, which raises the possibility of rights abuses and deficiencies in governance. More or less closely associated with regulatory capacity gaps, there are data ownership problem and technological dependency. The use of AI in surveillance or the early warning system depends on the availability of a significant amount of data and sophisticated analytical infrastructure. European institutions tend to have more influence over data ecosystems, technological design and system governance, which allows them to ensure that AI implementation is in line with regulatory and ethical standards. Conversely, the African peace and security organizations often depend on external technology, platforms and technical skills. The dependence does not only limit local control over information and system design, but also hinders possible institutional learning, adaptation, and sustainability. The reliance on external vendors and partners also contributes to the additional entrenchment of asymmetrical relations whereby African actors are more end users than co-producers of AI governance and innovation. The asymmetries in power as a norm setter in the global level support these structural inequalities. Europe is in a

privileged role of influencing the international discussion of AI ethics, regulation, and responsible use, and tends to globally disseminate its regulatory norms in the form of policy diffusion, development cooperation, and international alliances. Although these norms offer valuable points of reference to rights-based governance, their proliferation around the world may undermine alternative voices and contextual imperatives, especially of regions that face different security issues and institutional facts. Although African actors are becoming more vulnerable to the impacts of AI-enabled security interventions, they are still under-represented in global norm-setting processes, which restrict their powers in the rules and principles contributing to the technologies applied to their respective settings. These asymmetries of power and governance gaps highlight the weakness of the consistency of AI governance by or through uniform or transplant approaches to executive peace and security. They emphasize the necessity of governance systems that serve institutional capacity, enhance data sovereignty and enhance the inclusion of more participants in worldwide norm-setting. Placing AI in the context of larger systems of power and rule, this analysis preconditions a more critical approach to defining more balanced and context-aware strategies of Europe-Africa collaboration in the next section.

Conclusion and Policy-Oriented Position

The paper has examined how artificial intelligence should be governed in the context of peace and security based on a comparative example of Europe-Africa and found out that the level of the technological development does not define the outcomes of the AI-enabled surveillance, policing, and conflicts warning but the governance system does. The examples presented above demonstrate that AI is not a neutral tool of security improvement, but a power-structuring technology, the consequences of which are refracted through regulatory potential, institutional structure, and politics. In turn, the management of AI in the context of peace and security should be viewed as a political process in itself, but it is inherent in larger frameworks of authority, responsibility and inequality on a global scale. The comparative analysis indicates the endemic governance gap and power imbalance between Africa and Europe. The experiences of Europe demonstrate that the application of high-risk AI applications can be limited through legal frameworks, institutional control, and contestation opportunities and aligned with rights-based values. Conversely, several African settings are structurally constrained as represented by fragile regulatory capacity, inadequate data governance frameworks, and reliance on externally-created technologies. This situation poses greater risks of AI application to civil liberties, accountability, and sustainable peace outcomes. At the same time, these disparities are enhanced by the asymmetries in setting regional standards as global norms and ethics are often subjected to pressure exerted by the forces of the Global North, often without regard to the multiple security realities and institutional capabilities.

Policy-wise, these results highlight the shortcomings of policing strategies that are based on regulatory transplantation or one-way diffusion of norms. The effectiveness of the European regulatory models as reference points is subject to the institutional environments, which cannot be presumed across the regions. More practical solutions to governing AI in the context of peace and security are available in strategies that emphasise contextual sensitivity, institutional empowerment, and collaborative approaches. This means that in the Europe-Africa setting, we need to move beyond compliance and adoption-based frameworks to models of co-production, where African actors are substantially involved in defining the principles of governance, the data practices and accountability processes.

In summary, to promote responsible and effective AI governance to promote peace and security, reconsideration of current hierarchies in global technological governance are needed. Fair Europe-Africa collaboration should extend beyond technical help and regulatory exportation to confront the latent power dynamics, safeguard data sovereignty and encourage home-based governance capabilities.

References

1. Canova, G., & Simmler, M. (2024). Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind.
2. Czuba, K. (2025). Government Digital Surveillance in Africa. Governance, 38(4).
3. Ischak, N. (2022). The Spread of Chinese Surveillance Tools in Africa (pp. 32–49). Routledge eBooks.
4. Ishola, A. V., Anya, A. A., Anya, K. A., & Anya, E. K. (2025). Beyond Forecasting: Reimagining Early Warning Systems amid the Sahel Crisis for Sustainable Africa-EU Peacebuilding. African Journal of Humanities and Contemporary Education Research, 20(1), 134-146.
5. Jegede, E., & Ayuba, Z. (2025). Evaluating the effectiveness of digital communication platforms in enhancing conflict early warning and early response: a literature review. 1(1), 350–366.
6. Jili, B. M. (2022). Africa: regulate surveillance technologies and personal data. Visual Education, 607(7919), 445–448.
7. Kuhlmann, S. (2024). Government Use of Facial Recognition Technologies under European Law(pp. 127–138). Cambridge University Press.
8. Lynch, N. (2024). Facial Recognition Technology in Policing and Security—Case Studies in Regulation. Laws, 13(3), 35.
9. Mandokhail, A. W. K. (2024). The Transformative Role of Artificial Intelligence in Conflict Resolution and Peacekeeping. NUST Journal of International Peace and Stability, 104–109.

10. Muggah, R., & Whitlock, M. A. (2022). Reflections on the Evolution of Conflict Early Warning. Stability: International Journal of Security and Development, 10(1).
11. Noyes, A., & Yarwood, J. (2013). The AU Continental Early Warning System: From Conceptual to Operational? International Peacekeeping, 20(3), 249–262.
12. Osee, U. B. (2024). Integrating Artificial Intelligence: A Step towards the African Peace and Security Architecture. International Journal of Social Science Humanity & Management Research, 3(05).
13. Qandeel, M. (2024). Facial recognition technology: regulations, rights and the rule of law. Frontiers in Big Data, 7.
14. Roberts, T., Gitahi, J., Allam, P., Oboh, L., Oladapo, O., Appiah-Adjei, G., Galal, A., Kainja, J., Phiri, S., Abraham, K., Skelton, S. K., & Sheombar, A. (2023). Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia.
15. Selamet, M. S., Prakoso, L. Y., & Risahdi, M. (2025). Artificial Intelligence for Peace and Conflict Resolution. Indonesian Journal of Interdisciplinary Research in Science and Technology, 3(8), 847–858.
16. Souaré, I. K. (2007). Conflict prevention and early warning mechanisms in West Africa: A critical assessment of progress. African Security Review, 16(3), 96–109.
17. Zelizer, C., Ogenga, F., Schirch, L., Tauchnitz, E., Valenzuela, S., & Howard, P. N. (2025). Artificial Intelligence and Peacebuilding: Opportunities and Challenges.