Original Scientific Paper/Original naučni rad UDC/UDK: 17:004.8]:502/504
Paper Submitted/Rad primljen:31.12.2025.
Paper Accepted/Rad prihvaćen:10.01.2026.
DOI: 10.5937/SJEM2601061I

Iznad bojnog polja: Etičke implikacije i regulatorni izazovi korišćenja autonomnih AI sistema za bezbednost životne sredine i zaštitu resursa

Aleksandar Ivanov [1], Kire Babanoski[2], Vladimir M. Cvetković[3]

[1]Faculty of Security, Skopje, University “St. Kliment Ohridski”, Bitola, North Macedonia, aleksandar.ivanov@uklo.edu.mk
[2]Faculty of Security, Skopje, University “St. Kliment Ohridski” Bitola, North Macedonia, kire.babanoski@uklo.edu.mk
[3]University of Belgrade; Scientific and Professional Society for Risk Management, Serbia, vladimirkpa@gmail.com

Apstrakt: Kako veštačka inteligencija (AI) prelazi iz vojnih i industrijskih domena u nauku o životnoj sredini, fundamentalni zaokret ka metodologijama zasnovanim na podacima redefiniše zaštitu planete. Međutim, ova tranzicija često uvozi „logiku bojnog polja“ u očuvanje prirode, koristeći autonomne sisteme — kao što su dronovi i algoritmi mašinskog učenja — koji uvode složene etičke i regulatorne izazove. Ovaj rad predstavlja konceptualnu sintezu okvira veštačke inteligencije usmerene na čoveka (HCAI) i perspektiva ekološke bezbednosti kako bi se odgovorilo na ove rizike. Identifikujemo kritične tačke trenja, uključujući antropocentrične pristrasnosti koje zanemaruju dobrobit ne-ljudskih bića, jaz u odgovornosti u autonomnom donošenju odluka, narušavanje privatnosti putem nadzora i paradoksalni ekološki otisak AI računarstva. Da bismo ublažili ove rizike, predlažemo tri konkretne preporuke: uključivanje neantropocentričnih metrika u etičke standarde veštačke inteligencije; harmonizaciju prekograničnih regulatornih okvira radi usklađivanja sa globalnim standardima kao što je Akt o veštačkoj inteligenciji EU (EU AI Act); i obavezivanje na strogo definisane human-in-the-loop protokole (učešće čoveka u procesu odlučivanja) za sve autonomne intervencije u životnoj sredini.

Ključne reči: bezbednost životne sredine, autonomni AI sistemi, etika veštačke inteligencije, algoritamska regulacija, veštačka inteligencija usmerena na čoveka (HCAI), zaštita resursa.

Beyond the Battlefield: The Ethical Implications and Regulatory Challenges of Using Autonomous AI Systems for Environmental Security and Resource Protection

Abstract in English: As Artificial Intelligence (AI) transitions from military and industrial domains to environmental science, a fundamental shift toward data-driven methodologies is reshaping planetary protection. However, this transition frequently imports battlefield logic into conservation, utilizing autonomous systems—such as drones and machine learning algorithms—that introduce complex ethical and regulatory challenges. This paper presents a conceptual synthesis of Human-Centered AI (HCAI) frameworks and ecological security perspectives to address these risks. We identify critical friction points, including anthropocentric biases that neglect non-human wellbeing, a responsibility gap in autonomous decision-making, privacy infringements through surveillance, and the paradoxical environmental footprint of AI computing. To mitigate these risks, we propose three actionable recommendations: incorporating non-anthropocentric metrics into ethical AI standards; harmonizing transboundary regulatory frameworks to align with global standards like the EU AI Act; and mandating strictly defined human-in-the-loop protocols for all autonomous environmental interventions.

Keywords: Environmental Security, Autonomous AI Systems, AI Ethics, Algorithmic Regulation, Human-Centered AI (HCAI), Resource Protection.

1. Introduction

The integration of artificial intelligence (AI) into environmental sectors has catalyzed a profound shift in natural resource management, opening vast opportunities for improving efficiency, decision-making, and sustainability (Nizamani et al., 2025). This technological evolution is increasingly recognized as a vital mechanism for achieving the Sustainable Development Goals (SDGs), particularly regarding poverty alleviation, infrastructure development, and the protection of life on land (Chisom et al., 2024; Mhlanga, 2021; Vinuesa et al., 2020).

However, the application of these technologies is not value-neutral; it is contingent upon overarching security discourses that often mirror military logic (Francisco, 2023). As nations such as Kenya adopt AI and drones for major wildlife conservation reforms (The Standard, 2025), and conservation organizations deploy thermal cameras to protect rhinos (World Wildlife Fund, n.d.), we are witnessing a paradigm shift where the tools of the battlefield are being repurposed for environmental security. While these autonomous systems promise to maximize the potential of conservation data (Ahumada et al., 2019), they operate within a fragile ethical landscape. The rapid deployment of such agents raises critical questions regarding accountability and transparency (Bahrevar & Khorasani, 2021; Cheong, 2024), alongside the risk that algorithmic thinking may perpetuate hegemonizing knowledge or estrange us from ecological realities (Francisco, 2023).

Conservation AI requires governance that rejects militarized assumptions and centers ecological wellbeing, accountability, and transparent data practices. Section 2 outlines the methodology; Section 3 surveys capabilities and use cases; Section 4 analyzes ethical risks; Section 5 maps regulation to controls; and Section 6 concludes with practical recommendations.

2. Methodology

To analyze the intersection of autonomous systems, ethics, and environmental security, this paper employs a scoping review methodology complemented by illustrative case studies. This approach is designed to map rapidly evolving concepts across disparate fields—computer science, environmental law, and security studies—allowing for a comprehensive synthesis of current trends and policy gaps.

2.1. Search Strategy and Inclusion Criteria

Data collection prioritized high-quality sources published between 2019 and 2025. This timeframe was selected to capture the data-driven revolution in conservation and the emergence of significant regulatory frameworks such as the EU AI Act. The review integrates two primary categories of literature:

Peer-Reviewed Scholarship: Academic articles focusing on AI ethics, remote sensing, and ecological security to ensure theoretical rigor.

Reputable Policy & Technical Reports: Guidelines and white papers from authoritative bodies, including the Association for Computing Machinery (ACM), the European Commission, and major conservation NGOs (e.g., WWF, IUCN), to ground the analysis in real-world governance challenges.

2.2. Justification for Foundational Works

While the focus is on recent advancements, select foundational texts pre-dating 2019 are included to trace the lineage of current technologies. Works such as Hernandez (1990) on expert systems in law enforcement and Horswill (1995) on specialized real-time systems provide critical historical context, demonstrating how the current application of security logic to nature has deep roots in early computing and military adaptation.

2.3. Analysis and Synthesis

The selected literature was synthesized thematically to identify ethical friction points and regulatory voids. To bridge the gap between abstract theory and practice, the paper utilizes illustrative cases of deployed technologies—specifically the Wildlife Insights and EarthRanger platforms. These cases serve not as empirical data points, but as tangible examples of how autonomous agents are currently operationalizing security in the wild.

3. The Rise of Autonomous Environmental Security

Current environmental security technologies operate across a spectrum of autonomy, evolving from passive observation to active intervention. We propose the following taxonomy to categorize these systems:

1. Sensing: Passive data collection via camera traps, acoustic sensors, and thermal imaging.
2. Analytics: Machine learning models that perform classification (species identification) and prediction (poaching risk analysis).
3. Actuation: Autonomous or semi-autonomous physical agents, such as drones (UAVs) used for patrols or interdiction.
4. Decision Platforms: Integrated dashboards like EarthRanger that aggregate sensor data to direct human or automated responses.

3.1. Capabilities and Mini-Cases

Historically, environmental monitoring was characterized by significant time lags. Today, platforms maximize data potential through automation.

- Case A: Wildlife Insights (Analytics). This platform utilizes AI to process millions of camera trap images, transforming raw data into actionable biodiversity metrics and reducing analysis time from months to minutes (Ahumada et al., 2019).
- Case B: EarthRanger (Decision Support). This system integrates real-time data from radios, animal trackers, and sensors into a domain awareness dashboard, allowing rangers to deploy assets efficiently (Wall et al., 2024).
- Case C: Predictive Hotspot Alerts (Prediction). AI models analyze historical poaching data to predict crime hotspots. However, these incident histories often reflect biases from previous patrol patterns or reporting inequities rather than absolute crime distribution. Such systemic biases necessitate the rigorous audit trails and RACI accountability frameworks discussed later in this study to ensure fairness in deployment (Sustainability Directory, 2024).

3.2. The Intersection with Organized Crime

The militarization of conservation is partly a response to the sophistication of environmental crime. In Africa, the intersection of AI and organized crime presents a significant threat, necessitating advanced technological countermeasures. Specialized real-time systems are required to navigate these hostile environments. Yet, as Francisco notes (Francisco , 2022), this national security discourse can emphasize military uses of AI, potentially overshadowing human and ecological security needs.

4. Ethical Implications: The Logic of the Battlefield in Nature

This section explores the ethical friction points created when autonomous systems are deployed in complex social and ecological environments.

4.1. Anthropocentrism and Ecological Metrics

A major ethical deficiency in current AI deployment is its anthropocentric focus. AI ethics standards often prioritize human wellbeing while neglecting environmental wellbeing. This creates systemic vulnerability, where the rigid logic of AI systems may fail to grasp the complexity of biological ecosystems. To counter this, governance must include ecological metrics alongside human performance indicators. For example, while a persistent drone patrol may successfully reduce poaching, the acoustic disturbance could increase stress levels in sensitive non-target species. Consequently, projects should explicitly declare and monitor non-target species stress proxies, such as flight initiation distance and acoustic load, to ensure these trade-offs are effectively measured and governed.

4.2. The Responsibility Gap and RACI Mapping

The deployment of autonomous agents introduces a responsibility gap. If an autonomous system harms a local community member or makes an erroneous ecological decision (e.g., culling the wrong animals), determining accountability is difficult. To operationalize accountability, we propose a **RACI (Responsible, Accountable, Consulted, Informed)** mapping for the AI lifecycle:

- **Responsible (The "Doer"):** The Field Operations Lead ensures the AI is deployed according to protocol.
- **Accountable (The "Owner"):** The Project Principal Investigator (PI) or Park Warden retains ultimate liability for system outcomes. This role is specifically responsible for signing off on Fundamental Rights Impact Assessments (FRIAs) and post-incident reviews to ensure strict alignment with regulatory controls.
- **Consulted (Two-way communication):** Local Community Boards provide input on sensor placement and data privacy.
- **Informed (One-way communication):** Oversight Ministries receive regular audit reports.

4.3. Surveillance, Privacy, and Data Sovereignty

Surveillance technologies used for conservation can infringe on the collective right to access information and the privacy of local populations. Without ethical data governance, smart city surveillance tactics applied to nature reserves can lead to data colonialism, where information about local resources is extracted without local consent. Governance frameworks must adopt data sovereignty principles. This includes purpose limitation and the explicit operational rule that data collected for wildlife monitoring cannot be repurposed for unrelated commercial use without renewed consent.

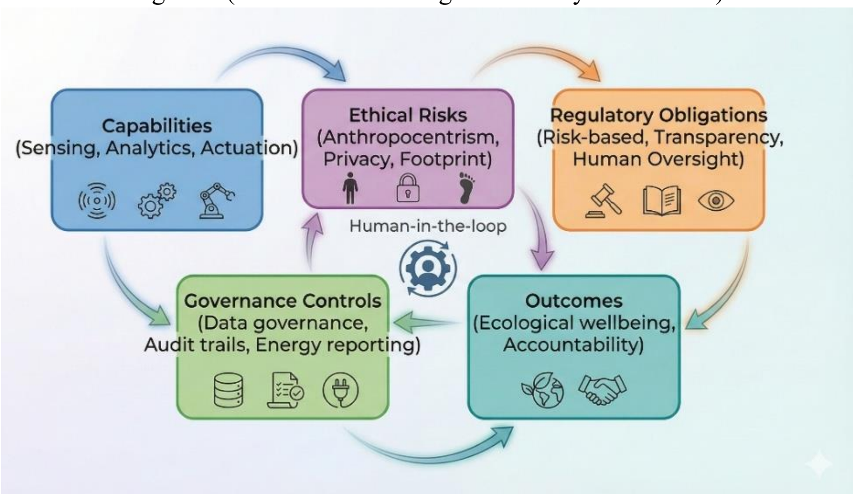
4.4. The Environmental Footprint of AI

Paradoxically, the AI systems used to protect the environment have a significant ecological footprint. Recent analyses indicate that most companies ignore the environmental impact of their AI operations. To be truly human-centered and sustainable, AI hardware must adhere to energy efficiency requirements. Practical controls include adaptive scheduling—retraining models only during off-peak energy hours—and favoring efficient edge-computing hardware over massive cloud reliance. Furthermore, energy and emissions reporting should be formally integrated into project documentation and subject to periodic audits.

5. Regulatory Challenges and Governance Frameworks

See Figure 1 for an overview of how capabilities map to risks, obligations, and controls.

Figure 1 (The HCAI × Ecological Security Framework)



Source: Visualization generated by Gemini (Google) based on conceptual frameworks and technical guidance provided by the authors.

The regulation of autonomous environmental systems is currently fragmented. While the United States moves toward a national framework, the **EU AI Act** represents the first comprehensive attempt to categorize AI based on risk. For environmental security, which often involves transboundary resources, this fragmentation is problematic. To operationalize intelligent regulation, we map the EU AI Act's risk categories to specific conservation use cases (Table 1).

To combat the opacity of proprietary black box algorithms, there is a growing movement toward open-source governance in environmental projects. However, transparency alone is insufficient; systems must be context-aware and accompanied by clear audit trails.

Table 1: Applying the EU AI Act[1] Risk Framework to Environmental Security

Risk Category	Conservation Use Case	Key Obligations	Practical Controls & Governance
Unacceptable Risk	**Social Scoring of Communities:** Using AI to rank local villagers based on resource usage or movement patterns.	**Prohibited.**	**Strict Ban:** Explicit policies forbidding the use of conservation data for social credit systems.
High Risk	**Predictive Policing & Interdiction:** Autonomous drones identifying "biometric or identity□linkable analytics in high□risk interdiction contexts" or predicting crime hotspots (Sustainability Directory, 2024).	**Strict Compliance:** Fundamental Rights Impact Assessment (FRIA), high data quality, human oversight.	**Human-in-the-Loop:** No autonomous engagement; human rangers must verify AI alerts. **Audit Trails:** Logs of all AI predictions vs. outcomes.
Limited Risk	**Biometric Monitoring (Wildlife):** Automated species identification via camera traps (e.g., Wildlife Insights).	**Transparency:** Users must know they are interacting with AI (if applicable).	**Data Governance:** Open-source verification of species classifiers to prevent bias (Meegle, 2025).
Minimal Risk	**Environmental Modeling:** AI used for analyzing soil samples or deforestation trends (Gizachew, 2025).	**Voluntary Codes of Conduct.**	**Open Science:** Sharing models and datasets to foster trust and reproducibility.

6. Conclusion

The transition of AI beyond the battlefield into environmental security offers a powerful mechanism for resource protection. However, as this paper has demonstrated, it is fraught with ethical and regulatory perils. Drawing on the Human-Centered AI framework and ecological security perspectives, it is clear that technological solutions cannot be divorced from their socio-political contexts.

To ensure these systems are sustainable, we recommend:

1. *Ecological Ethics:* Incorporate non-anthropocentric metrics into AI standards to respect the wellbeing of the ecosystem itself.
2. *Harmonized Regulation:* Align transboundary monitoring projects with global standards like the EU AI Act to prevent regulatory arbitrage.
3. *Mandatory Human Oversight:* Enforce strictly defined human-in-the-loop protocols for all high-risk autonomous interventions.

Future research should prioritize operationalizing participatory audits, developing indigenous and community-led data governance models, and launching cross-border interoperability pilots to harmonize transboundary resource protection. Only by addressing these challenges can we harness the power of AI to protect our planet without replicating the logic of conflict that birthed these technologies.

Appendix: Operational Governance Toolkit
A. Fundamental Rights Impact Assessment (FRIA) for Environmental AI
This assessment is mandatory for "High-Risk" systems, such as predictive policing or autonomous interdiction drones, to ensure compliance with human rights and ecological integrity, as mandated by emerging standards like the EU AI Act.

[1] https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (This regulation establishes the harmonized rules and risk-based framework mentioned in your paper's analysis of environmental security governance. As outlined in your manuscript, this act categorizes AI systems into risk levels (unacceptable, high, limited, and minimal), which serves as the foundation for the "Risk-to-Control" mapping used in your study.)

• **Project Title & ID: [e.g., Project Rhino-Shield Alpha]**
• **System Description: Briefly describe the autonomous agent, its sensing capabilities, and the level of autonomy in actuation.**
• **Intended Purpose: Define the specific environmental security goal (e.g., identifying illegal logging in Sector 7).**
• **Targeted Populations: Identify human communities (indigenous groups, local villagers) and non-target biological species potentially impacted by the system's presence.**
• **Risk Assessment:**
○ **Privacy & Surveillance: Does the system capture identity-linkable data that may infringe on the collective right to access information?**
○ **Algorithmic Bias: Are the training datasets representative of local realities to prevent environmental injustice?**
○ **Ecological Disturbance: What is the predicted acoustic load or physical intrusion for sensitive non-target species?**
• **Mitigation Strategy: Describe the human-in-the-loop protocols and privacy masking techniques deployed to maintain meaningful human control.**
B. Environmental AI Model Card (Short Form)
A standardized document to combat the opacity of "black box" proprietary algorithms by detailing the model's performance, limitations, and normative groundings.
• **Model Developer: [e.g., University Conservation Tech Lab]**
• **Model Version & Date: [e.g., v2.1, October 2025]**
• **Model Type: Specify the architecture (e.g., Convolutional Neural Network for species classification).**
• **Training Data: List primary datasets used and their origin to ensure data sovereignty.**
• **Performance Metrics: Accuracy, precision, and recall rates across varied environmental conditions (e.g., night-time vs. day-time performance).**
• **Ecological Constraints: Explicitly state environmental conditions where the model fails (e.g., high failure rate during heavy tropical rainfall).**
C. Dataset Information Sheet
Ensures transparency in data governance and prevents "data colonialism" by documenting the origin and consent status of data.
• **Data Source: (e.g., Community-monitored sensors in Reserve X).**
• **Collection Method: (e.g., Automated passive acoustic monitoring).**
• **Consent & Sovereignty Status: Confirmation that local community boards have signed off on data collection processes.**
• **Purpose Limitation Rule: Explicit declaration that data collected for wildlife monitoring cannot be repurposed for unrelated commercial use without renewed community consent.**
• **Data Retention: Schedule for when identity-linkable analytics will be anonymized or deleted.**
D. Operational Accountability & Sustainability Logs
These logs provide a transparent audit trail for regulators and oversight bodies to bridge the responsibility gap.
D.1 Incident Response Log (Audit Trail)
• **Timestamp: [YYYY-MM-DD HH:MM]**
• **Autonomous Alert: (e.g., "Potential human intrusion detected in restricted zone").**
• **Human Verification: (e.g., Ranger verified via thermal link).**
• **Outcome: (e.g., "Confirmed false positive – local resident collecting fallen wood; system updated to recognize traditional tool signatures").**
• **Sign-off: [Ranger ID] to ensure individual and collective accountability.**
D.2 Energy & Emissions Log (Sustainability Reporting)
• **Reporting Period: [e.g., Q4 2025]**
• **Compute Energy Usage: Total kWh consumed for model training and edge-cloud operations.**
• **Carbon Footprint: Estimated CO2e based on the local energy grid and hardware lifecycles.**
• **Efficiency Measures: (e.g., "Model retraining restricted to off-peak renewable energy hours").**

Statement

During the preparation of this work the author(s) used Gemini (Google) in order to assist with the visualization of conceptual frameworks and to provide suggestions for the structural organization of the manuscript. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

References

1. Ahumada, J. A., Fegraus, E., Birch, T., Flores, N., Kays, R., O'Brien, T. G., … Dancer, A. (2019). Wildlife Insights: A Platform to Maximize the Potential of Camera Trap and Other Passive Sensor Wildlife Data for the Planet. Environmental Conservation, 47 (1), 1–6. doi: 10.1017/S0376892919000298
2. Association for Computing Machinery. (2018). ACM Code of Ethics and Professional Conduct. New York: ACM Council.
3. Bahrevar, R. & Khorasani, K. (2021). Accountability and Transparency in AI Systems: A Public Policy Perspective. (Unpublished thesis). Concordia University, Montreal, Canada.
4. Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. & Winfield, A. (2020). The Ethics of Artificial Intelligence: Issues and Initiatives. European Parliament Panel for the Future of Science and Technology (STOA). doi: 10.2861/6644
5. Buiten, M. (2019). Towards Intelligent Regulation of Artificial Intelligence. European Journal of Risk Regulation, 10 (1), 41–59. doi: 10.1017/err.2019.8
6. Cheong, B. C. (2024). Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making. Frontiers in Human Dynamics, 6, 1421273. doi: 10.3389/fhumd.2024.1421273
7. Chisom, O. N., Biu, P. W., Umoh, A. K., Obaedo, B. O., Adegbite, A. O. & Abatan, A. (2024). Reviewing the Role of AI in Environmental Monitoring and Conservation: A Data-Driven Revolution for our Planet. World Journal of Advanced Research and Reviews, 21 (01), 161–171.
8. Conservation International. (2020). Wildlife Insights Platform Feature Build-out, Support and Maintenance. Retrieved on 23 December 2025, from [Insert URL if available]
9. Crowell & Moring. (Days 19 December 2025). Executive Order Tries to Thwart "Onerous" AI State Regulation, Calls for National Framework. [Journal/Portal Name].
10. Dalton, D., Berger, V., Kirchmeir, H., Adams, V., Botha, J., Halloy, S., … Jungmeier, M. (2024). A Framework for Monitoring Biodiversity in Protected Areas and Other Effective Area-Based Conservation Measures: Concepts, Methods and Technologies. IUCN WCPA Technical Report Series No. 7. Gland: IUCN. doi: 10.2305/HRAP7908
11. Data Privacy Brasil. (Days 31 October 2025). Artificial Intelligence, Sustainability and the Collective Right to Access Information. Retrieved on 23 December 2025, from
12. ENACT Africa. (Days 29 June 2023). AI and Organised Crime in Africa. Retrieved on 23 December 2025
13. European Commission. (2025). Answers for WildEuro - MSCA 101107666. Documents Download Module.
14. European Parliament. (2023). EU AI Act: First Regulation on Artificial Intelligence. Retrieved on 23 December 2025, from https://www.europarl.europa.eu/
15. Francisco, M. (2023). Artificial Intelligence for Environmental Security: National, International, Human and Ecological Perspectives. Current Opinion in Environmental Sustainability, 61, 101250. doi: 10.1016/j.cosust.2022.101250
16. Gaulin, M. (2024). New Analysis Finds Most Companies Ignore AI Environmental Impact. Lab Manager. Retrieved on 23 December 2025
17. Gizachew, B. (2025). AI and Machine Learning in Remote Sensing for Tropical Forest Monitoring: Applications, Challenges, and Emerging Solutions. Preprints.org. doi: 10.20944/preprints202512.1554.v1
18. Global Affairs Canada. (2019, June). Ethical and Methodological Framework for Open Source Data Monitoring and Analysis. Ottawa: Government of Canada.
19. Goel, P. K., Saifi, S., Goel, N. & Aeron, S. (2025). Ethical Considerations in AI: Applications for Wildlife Conservation. In AI and Machine Learning Techniques for Wildlife Conservation (pp. 247–266). Hershey: IGI Global. doi: 10.4018/979-8-3693-6935-7.ch010

20. Gupta, A. & Kaur, R. (2025). Role of AI Powered Drones and Satellite Imagery in Detecting Poaching Activities. International Journal of Research Publication and Reviews, 6 (10), 7097–7110. doi: 10.55248/gengpi.06.1025.3836
21. Hernandez, A. P. (1990). Artificial Intelligence and Expert Systems in Law Enforcement: Current and Potential Uses. Computers, Environment and Urban Systems, 14, 299–306.
22. Hohma, E., Boch, A., Trauth, R. & Lütge, C. (2023). Investigating Accountability for Artificial Intelligence Through Risk Governance: A Workshop-Based Exploratory Study. Frontiers in Psychology, 14, 1073686. doi: 10.3389/fpsyg.2023.1073686
23. Horswill, I. (1995). Analysis of Specialized Real-Time Systems. Artificial Intelligence, 73 (1–2), 1–30.
24. Johann Heinrich von Thünen Institute. (2025). Assessing the Suitability of Available Global Forest Maps as Reference Tools for EUDR-compliant Deforestation Monitoring. Remote Sensing, 17 (17), 3012. doi: 10.3390/rs17173012
25. Jones, R. K. (2026). Ethical Considerations in Deploying Autonomous AI. In Safeguarding and Securing Autonomous AI Agents (pp. 133–170). Hershey: IGI Global Scientific Publishing. doi: 10.4018/979-8-3373-6876-4.ch005
26. Kingston, J. (2017). Using Artificial Intelligence to Support Compliance with the General Data Protection Regulation. International Journal of Law and Information Technology, 25 (3), 226–243.
27. Loisaba Conservancy. (n.d.). Security. Retrieved on 23 December 2025, from https://www.loisaba.com/
28. Maitra, S., Lang, L. & Hernández Jurado, M. (n.d.). How Shifting Responsibility for AI Harms Undermines Democratic Accountability. Retrieved on 23 December 2025
29. Meegle. (Days 23 October 2025). Open-source Governance in Environmental Projects. Retrieved on 23 December 2025
30. Mhlanga, D. (2021). Artificial Intelligence in the Industry 4.0, and its Impact on Poverty, Innovation, Infrastructure Development, and the Sustainable Development Goals: Lessons from Emerging Economies? Sustainability, 13, 5788. doi: 10.3390/su13115788
31. Microavia. (n.d.). How Drones are Used in Wildlife Monitoring to Protect Against Poaching. Retrieved on 23 December 2025, from https://microavia.com/
32. Moreno, N. & McAllister Novak, A. (Days 21 January 2025). Key Insights into AI Regulations in the EU and the US: Navigating the Evolving Landscape. Kennedys Law LLP.
33. Nizamani, M. M., Zhang, H. L. & Lai, Z. (2025). Human-centered AI: Advancing Ethical, Transparent, and Context-aware Systems for Sustainable Development. Technology in Society, 80, 103121. doi: 10.1016/j.techsoc.2025.103121
34. NVIDIA. (2025). NVIDIA Sustainability Report Fiscal Year 2025. Retrieved on 23 December 2025
35. Ojija, F., Ogwu, M. C., Ally, J., John, J. P., Stephano, A., Felix, N. & Tekka, R. (2025). Artificial Intelligence-driven Solutions for Mitigating Human–Wildlife Conflict in Biodiversity Hotspots. Public Health Reviews, 108 (4). doi: 0.1177/00368504251394584
36. Prokopowicz, D. (2025). The Use of Big Data and Artificial Intelligence in Protecting the Climate and Biodiversity of Planet Earth. Warsaw: Cardinal Stefan Wyszynski University. doi: 10.13140/RG.2.2.23721.25446
37. Rigley, E., Chapman, A., Evers, C. & McNeill, W. (2023). Anthropocentrism and Environmental Wellbeing in AI Ethics Standards: A Scoping Review and Discussion. AI, 4, 844–874. doi:10.3390/ai4040043
38. Scoble, R. & Cronin, I. (Days 24 June 2025). How AI is Revolutionizing Wildlife Conservation. Unaligned Newsletter.
39. Serry, E. (2025). Ethical Implications of Artificial Intelligence: Challenges, Risks, and Regulatory Perspectives. (Unpublished thesis). Teesside University, UK. doi: 10.13140/RG.2.2.11350.56645
40. Shahrouz, M., Nazari, A. & Moradi, S. (2023). AI-driven Cybersecurity: Legal and Ethical Considerations in Autonomous Systems Protecting Digital Networks. Legal Studies in Digital Age, 2 (1), 1–12.
41. Stahl, B. C. (2023). Responsible AI: From Principles to Implementation and Regulation. Scientific Reports, 13, 34622. doi: 10.1038/s41598-023-34622-w
42. Stahl, B. C. (2025). The Ethics of Data and its Governance: A Discourse Theoretical Approach. Information, 16 (6), 497. doi: 10.3390/info16060497
43. Sustainability Directory. (2024a). AI for Wildlife Crime Prediction. Retrieved on 23 December 2025

44. Sustainability Directory. (2024b). Ethical Data Governance. Retrieved on 23 December 2025
45. Sustainability Directory. (2024c). Ethical Frameworks for Smart City Surveillance. Retrieved on 23 December 2025
46. Sustainability Directory. (2024d). To what Extent Does Data Privacy Relate to Global Sustainability Goals? Retrieved on 23 December 2025
47. Sustainability Directory. (n.d.). Ethical Implications of AI in Water Resource Management. Retrieved on 23 December 2025
48. Terenzio, F. (2025). Systemic Vulnerability: From AI Systems to Environmental Systems. Topoi. doi: 10.1007/s11245-025-10285-2
49. The Standard. (Days 23 December 2025). Kindiki: Kenya Adopts AI, Drones in Major Wildlife Conservation Reforms. The Standard.
50. TRENDS Research & Advisory. (2024). The Backlash Against Military AI: Public Sentiment, Ethical Tensions, and the Future of Autonomous Warfare. Abu Dhabi: TRENDS.
51. University of Cambridge. (n.d.). AI and Conservation Resolution Adopted at the IUCN World Conservation Congress. Retrieved on 23 December 2025
52. VERSO. (n.d.). Ethics - Introduction. Open Resource Library. Retrieved on 23 December 2025
53. Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., … Fuso Nerini, F. (2020). The Role of Artificial Intelligence in Achieving the Sustainable Development Goals. Nature Communications, 11, 233. doi: 10.1038/s41467-019-14108-y
54. Wall, J., Lefcourt, J., Jones, C., Doehring, C., O’Neill, D., Schneider, D., … Wittemyer, G. (2024). EarthRanger: An Open-source Platform for Ecosystem Monitoring, Research and Management. Methods in Ecology and Evolution, 15 (11), 1968–1979. doi: 10.1111/2041-210X.14399
55. White & Case LLP. (2025). Energy Efficiency Requirements Under the EU AI Act. Retrieved on 23 December 2025, from https://www.whitecase.com/
56. Winter, J. S. & Davidson, E. (2019). Governance of Artificial Intelligence and Personal Health Information. Digital Policy, Regulation and Governance. doi: 10.1108/DPRG-08-2018-0048
57. World Resources Institute. (2025a). Terms of Service - WRI Data Platforms. Retrieved on 23 December 2025, from https://www.wri.org/
58. World Resources Institute. (2025b). WRI's Approach to Responsible Artificial Intelligence. Washington: WRI.
59. World Wildlife Fund. (n.d.). Thermal Cameras and AI Help Protect Rhinos in Kenya. Retrieved on 23 December 2025, from https://www.worldwildlife.org/
60. Yehudi, Y., Bennett, A., Turon, G., Bays, D., Gibson, S., Druskat, S., … Batchelor, S. (2022). Ethical Considerations When Choosing an Open Source Governance Model. The Turing Way. doi: 10.5281/zenodo.6144158