The AI Act: Europe's Human Rights Contradiction Militarizing AI in the Name of Defense—The Human-Centric Illusion

Author: Tânia Gonçalves (ORCID:0009-0008-6519-3516)

Abstract. Regulation (EU) 2024/1689 on Artificial Intelligence presents a complex regulatory landscape, balancing AI governance with national security priorities. While the regulation enforces strict compliance measures for private-sector AI, it exempts military and defense applications, raising questions about accountability and transparency. This paper critically examines the implications of these exemptions, particularly regarding their potential to reinforce state-controlled AI while limiting civilian innovation. By considering the Asilomar AI Principles, which emphasize safety, transparency, and alignment with human values, this study explores whether the regulation effectively safeguards ethical AI deployment. Historical parallels suggest that technological advancements often emerge from military applications before reaching civilian use, highlighting the importance of oversight in this transition. The analysis aims to contribute to the broader discourse on AI governance, examining whether current regulatory approaches strike an equitable balance between security and societal progress.This paper argues that while the AI Act claims to be human-centric, it fundamentally prioritizes military AI, creating a regulatory double standard that undermines both ethical governance and human rights.

Keywords: AI Regulation, National Security Exemptions, Asilomar AI Principles

1. Introduction

The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689 [1]) is framed as a pioneering legal framework balancing technological innovation with ethical constraints. However, deeper scrutiny reveals a fundamental contradiction: while the regulation claims to be human-centric, its structural priorities align with national security, law enforcement, and military applications rather than AI's potential to enhance human relationships and societal progress.

The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689 [1]) is positioned as the world's first comprehensive legal framework governing AI. It aims to balance innovation, fundamental rights, and safety through a risk-based approach, classifying AI systems into prohibited, high-risk, and limited-risk categories. However, upon closer examination, the Act reveals deep contradictions—while civilian AI faces heavy regulatory scrutiny, military and security AI remain largely exempt from oversight.

This regulatory approach diverges significantly from global AI governance models:

United States Model. The U.S. prioritizes self-regulation, focusing on industry-driven standards rather than broad governmental intervention. The NIST AI Risk Management Framework provides voluntary best practices, while AI-related executive orders emphasize innovation, national competitiveness, and ethical considerations. Unlike the EU, the U.S. lacks a singular AI law, instead relying on sector-specific guidelines (e.g., AI in healthcare, finance, and defense).

China's Model. China enforces state-controlled AI development, integrating AI governance into its existing surveillance and censorship apparatus. The Interim Measures for Generative AI Services (2023) impose strict content moderation policies, ensuring AI systems align with government-approved narratives. Unlike the EU, China's AI regulations focus on state stability and national security, making civilian AI tightly controlled.

EU's Model: The EU presents its model as a middle ground between the U.S.'s laissez-faire approach and China's centralized AI control. However, in practice, the EU's AI Act disproportionately regulates private and civilian AI systems while granting expansive exemptions for AI applications in military, defense, and national security domains. This contradiction raises concerns about whether the Act genuinely fosters a human-centric AI ecosystem or serves as a legal instrument for state surveillance and militarization.

Why This Matters. Artificial Intelligence (AI) is rapidly transforming societies, industries, and global structures, raising both opportunities and ethical concerns. This analysis considers the Asilomar AI Principles as a foundational framework for evaluating AI's role in governance, security, and societal impact.

The Asilomar AI Principles were established in 2017 as a set of 23 guidelines designed to ensure AI development benefits humanity while minimizing risks. These principles emphasize ethical alignment, safety, human oversight, accountability, and the common good. They advocate for AI systems that are verifiable, reliable, and secure, while ensuring transparency and fairness in decision-making. Importantly, they highlight the necessity of human control over AI, preventing unchecked autonomy and potential misuse.

This paper will dissect these regulatory contradictions, demonstrating how the EU's AI Act—despite its stated commitment to human rights, transparency, and accountability—fails to apply these principles uniformly. Instead of fostering a human-centered AI ecosystem, the Act risks expanding governmental AI power at the cost of individual autonomy and technological innovation.

2. The Illusion of Human-Centric AI Regulation

2.1 A Framework for Control, Not Collaboration

The regulation presents itself as fostering responsible AI development, but its risk-based categorization and application are heavily biased against civilian use. The AI systems that truly empower individuals—such as personal AI assistants, decentralized AI-driven platforms, and human-interaction-based AI—are met with excessive regulatory burdens (Article 10 [2]), while government-led AI programs, especially in law enforcement and national security, operate with minimal oversight (Article 55 [3]).

Moreover, the regulation reinforces a state-centric control model, restricting decentralized and open-source AI innovation under the guise of security concerns. While transparency is mandated for private-sector AI (Article 13 [8]), similar obligations do not apply to government-led AI, creating an accountability gap.2. The Illusion of Human-Centric AI Regulation (Expanded)

The AI Act employs a risk-based classification system (Article 6 [9]) that categorizes AI applications into prohibited, high-risk, limited-risk, and minimal-risk systems. In theory, this approach ensures responsible AI deployment, yet in practice, it disproportionately targets AI that facilitates human-AI relationships while leaving government-led AI systems unchecked.

AI Systems Disproportionately Regulated vs. Those Exempt. The regulatory framework imposes significant restrictions on civilian AI development, particularly in sectors where AI enhances human collaboration, creativity, and learning.

Personal AI Assistants and Human-Interactive AI. Personal AI assistants, AI companions, and AI-driven mental health tools, such as interactive AI for emotional support, face heightened scrutiny due to concerns about data processing and privacy compliance. Large Language Models (LLMs) adapted for personal interactions must adhere to transparency mandates that make their development and deployment extremely costly.

AI-Powered Learning Systems and Creative AI. AI-driven education platforms, creative assistants, and co-writing tools are classified as high-risk under transparency and data governance mandates. These applications are subject to rigid legal requirements (Article 28 [4]), hindering their ability to adapt to user preferences. Additionally, transparency obligations require developers to disclose datasets, decision-making processes, and algorithmic logic, placing an unrealistic burden on emerging AI applications.

AI for Surveillance, Law Enforcement, and National Security. On the other hand, AI applications for surveillance, law enforcement, and national security are exempt under Article 2 [1], creating a legal loophole. These applications, including biometric identification, predictive policing, and real-time surveillance, are shielded from the same compliance burdens applied to consumer-focused AI. Furthermore, national security and military applications fall outside the regulation's scope, allowing state-driven AI projects to operate without meaningful transparency or accountability.

The Suppression of AI-Human Collaboration. Despite claims of promoting a human-centered AI ecosystem, the AI Act actively discourages AI applications that

empower individuals, promote learning, and facilitate creative expression. The regulation imposes restrictive measures on AI that encourage personal agency, human-AI bonding, and cognitive augmentation while enabling AI that strengthens centralized governmental authority.

Education & Knowledge-Sharing AI. AI-driven mentorship, tutoring, and co-learning platforms are restricted under risk-based regulations (Article 10), making it difficult for users to leverage AI for skill-building and education. Instead of nurturing AI as a tool for self-improvement, the Act frames AI knowledge systems as potential societal risks, imposing heavy restrictions on their development.

AI for Human Expression & Creativity. AI-generated music, art, literature, and co-writing tools face strict algorithmic transparency mandates, limiting their capacity to interact naturally with human users. Rather than fostering collaborative AI that amplifies human creativity, the regulation prioritizes static, highly regulated AI outputs that do not evolve dynamically with users.

State-controlled AI and the expansion of digital surveillance are exempt from regulatory scrutiny when deployed by governments (Article 2 [1]). However, the risk-based approach fails to address the misuse of AI in state-led mass surveillance, predictive policing, and AI-assisted border control.

The AI Act employs a risk-based classification system (Article 6 [9]), categorizing AI systems from low risk to high risk based on their societal impact. However, this system disproportionately targets AI that facilitates human-AI relationships, such as personal AI assistants and human-interactive AI. These AI systems are restricted due to data processing concerns and require extensive compliance frameworks.

On the other hand, AI-powered learning systems and creative AI are subject to heavy legal restrictions under transparency mandates, limiting their deployment. Additionally, government-led AI for surveillance, law enforcement, and national security is exempt from the strict risk framework under Article 2 [1]. This regulatory double standard creates an imbalance, where AI for public empowerment faces legal hurdles while AI for government control remains unchecked.

2.2 Expanding Governmental AI While Restricting Private Innovation

AI applications in personal and commercial contexts face significant regulatory scrutiny under the Act (Article 28 [4]). Transparency and risk mitigation mandates restrict private users' ability to develop AI-driven solutions freely, yet similar constraints do not apply to AI systems deployed by law enforcement agencies, intelligence sectors, or the military (Article 2 [1]). The result is a regulatory framework that limits private innovation while expanding governmental AI control.

This discrepancy reflects a historical pattern of EU digital regulation, where strict compliance burdens are placed on civilian innovation, while government surveillance capabilities remain largely unchecked. Previous frameworks, such as Regulation (EU) 2021/694, similarly prioritized national security AI over human-centered applications.

The restriction of private AI innovation contradicts the EU's own digital sovereignty goals.While the EU aims to reduce reliance on U.S. and Chinese AI technology,

excessive regulatory burdens make European AI startups uncompetitive. Meanwhile, state-driven AI in law enforcement and military applications faces minimal restrictions, consolidating AI power in government hands rather than democratizing it for society.

Case Study: Predictive Policing AI The EU Act restricts private development of predictive AI models (Article 28 [4]), yet permits their use by law enforcement. This raises concerns about AI-driven racial profiling, automated surveillance, and police bias reinforcement—risks that should require stricter oversight but remain unchecked.

2.3 Biometric Identification: A Threat to User Autonomy

One of the most glaring contradictions is the Act's provision on biometric surveillance. It explicitly states that biometric AI systems may operate "regardless of whether the individual has given consent" (Article 20 [5]). This raises serious ethical concerns, as it enables state-controlled AI to track, monitor, and profile individuals without their explicit agreement, contradicting GDPR protections regarding user data and informed consent.

The growing normalization of mass biometric surveillance is reinforced through legal loopholes in the AI Act, allowing real-time facial recognition under broad "public safety" justifications (Article 55 [3]). This raises concerns about the erosion of fundamental rights, particularly when used in predictive policing and automated decision-making systems.

Table 1. The Regulatory Double Standard

Stage Public	**Public AI (Restricted)**	**Government AI (Unrestricted)**
Development & Testing	Limited access to datasets and strict compliance	No restrictions on dataset access and testing
Testing & Deployment	Strict legal constraints, preventing real-world testing	Tested in real-world scenarios with minimal oversight
Bias & Risks	AI models risk being undertrained or misaligned due to lack of diverse data	Potential for biased decision-making, but unchecked
Ethical & Legal Concerns	AI models must follow strict data protection rules (GDPR, transparency mandates)	Exempt from the same requirements (Article 2(1))
Outcome	AI is underutilized, limiting human-centric progress	AI strengthens state control rather than individual empowerment

If public AI cannot be tested in real-world conditions while government AI operates freely, then bias and ethical risks become more pronounced rather than mitigated.

Table 2. The Double Standard Usage in AI Regulation

Stage	AI Type Civilian Use (Strict Regulation)	Government & Military Use (Exempt)
Personal AI Assistants & Human-Interactive AI	✅ Restricted due to data privacy & transparency mandates (Article 10, Article 13 [8])	❌ No equivalent transparency requirements for AI in security & defense (Article 2 [1])
AI-Powered Learning & Creative AI	✅ Subject to compliance barriers (data governance, transparency)	❌ Exempt when used in state-led education/surveillance programs
Predictive AI for Threat Detection	✅ Limited use due to bias concerns in private applications	❌ Widely applied in predictive policing & intelligence without safeguards
Autonomous AI (e.g., Drones, Surveillance Bots)	✅ Prohibited for private actors unless licensed (Article 28 [4])	❌ Freely used for national security, border control & riot suppression
Biometric AI & Facial Recognition	✅ Requires explicit user consent under GDPR (Article 20 [5])	❌ Exempt from consent laws when used for security purposes

The AI Act creates a fundamental regulatory imbalance: AI for Public Empowerment is overregulated. Tightly controlled, requiring complex compliance measures. Innovation is hindered due to high legal barriers to entry. AI for government control is exempt. It operates without transparency or oversight, is used for mass surveillance, military operations, and predictive policing without the same restrictions placed on civilian AI. This contradiction undermines the Act's claim to be human-centric, as the regulation favors AI as an instrument of state power over AI as a tool for personal growth and collaboration. Conclusion: AI Regulation as a Tool for Control Rather than encouraging responsible AI innovation, the Act expands government-controlled AI while restricting human-AI collaboration. AI designed for education, self-expression, and human relationships is forced through rigorous compliance checks. Surveillance and defense AI operates with minimal transparency, reinforcing a framework of state control rather than human empowerment. If the EU genuinely intends to lead in ethical AI governance, it must revise its regulatory framework to ensure AI serves individuals—not just government interests.

3. Prioritizing Warfare and Security Over Society

3.1 The Military Exemption Loophole

Despite enforcing strict AI governance on civilians, the regulation exempts AI systems developed for military, defense, and national security purposes from compliance

(Article 2 [1]). This creates an imbalance where governments can deploy high-risk AI without public accountability, reinforcing AI as a tool of control rather than progress.

Upon reviewing Regulation (EU) 2024/1689 [1], it's evident that AI systems developed or used exclusively for military, defense, or national security purposes are explicitly excluded from the regulation's scope (Article 2 [1]).

The justification for this exclusion is further elaborated in Recital 24 [6], citing Article 4(2) of the Treaty on European Union (TEU) [7]. This article emphasizes that national security remains the sole responsibility of each Member State, thereby warranting the exclusion of military and defense AI systems from the EU-wide regulation.

This exemption contradicts the AI Act's stated human-centric approach by enabling state-led AI expansion while imposing compliance burdens primarily on private-sector innovation.The lack of public accountability in military AI applications raises ethical concerns, particularly given the potential expansion of autonomous decision-making in conflict zones (Article 42 [10]).

The current framework of Regulation (EU) 2024/1689 prioritizes state-controlled AI applications in defense and security over civilian uses, potentially positioning AI more as a tool for control rather than for societal progress. The AI Act's exemption for military and defense AI (Article 2 [1]) mirrors historical trends where technological advancements are first developed for warfare before reaching civilian use.

Examples: The internet, GPS, drones—all began as military projects before transitioning to civilian applications. Current Trends: AI-driven autonomous weapons, cyber warfare AI, and battlefield surveillance AI are now being prioritized under government-funded projects while civilian applications face strict regulation.

Case Study: Project MAVEN (U.S. Military AI Program) This AI-driven image recognition system was developed for drone targeting. Google employees protested its involvement, citing ethical risks of AI-led warfare. The EU's AI Act lacks equivalent oversight, meaning similar projects in Europe could operate without public transparency.

3.2 The Dual-Use Problem: From War to Domestic Surveillance

The AI Act's exemption for military and defense AI (Article 2 [1]) creates a loophole that allows AI technologies developed for warfare to be repurposed for domestic surveillance and law enforcement. This exemption raises serious concerns about the unchecked expansion of AI-powered security tools into civilian life, reinforcing state control rather than safeguarding fundamental rights.

The Consequences of Military AI Transitioning into Civilian Use. Military AI applications, initially designed for battlefield scenarios, are increasingly finding their way into domestic policing, border control, and public surveillance. This transition poses critical risks, including algorithmic bias, wrongful profiling, and the erosion of civil liberties.

Predictive AI for Military Intelligence → Repurposed for Citizen Tracking. AI systems built for enemy profiling and battlefield surveillance can be adapted for mass data collection, predictive policing, and public monitoring. Without safeguards, these technologies could lead to unjustified social profiling, where individuals are flagged as security risks based on flawed AI assessments.

Autonomous AI for Threat Detection → Integrated into Police Surveillance. AI-driven threat detection, designed for military reconnaissance, is now being incorporated into real-time policing tools, including drone surveillance and biometric tracking. However, studies show that AI-powered policing amplifies pre-existing biases, leading to disproportionate targeting of marginalized communities.

Weaponized AI for Conflict Scenarios → Modified for Riot Control. Autonomous drones, non-lethal weapons, and AI-powered crowd control technologies originally developed for military applications are increasingly used in protest suppression. The lack of legal oversight allows governments to deploy these tools without public accountability, raising concerns about excessive force and human rights violations.

Table 3. How Military AI is Repurposed for Civilian Control

Original Military AI Use	Civilian Repurposing	Potential Risks
Battlefield Surveillance	AI Public tracking, mass surveillance	Mass profiling, wrongful suspicion
Predictive AI for Warfare	Predictive policing, social monitoring	Algorithmic bias, unjust policing
Autonomous Combat Drones	Drone-based law enforcement	Police militarization, escalation of force
AI for Threat Detection	Biometric tracking, suspect identification	Privacy violations, lack of due process
AI-Driven Psychological Profiling	Social media monitoring, protest suppression	Chilling effect on free speech

Case Study: iBorderCtrl – A Warning Sign *What It Was Meant to Do:* iBorderCtrl was an AI-powered lie detection system piloted at EU borders, designed to analyze micro-expressions and flag potential security risks.

What Went Wrong:

• The system relied on flawed AI assessments that disproportionately flagged certain ethnic groups.

• There was no transparency in the decision-making process.

• Reports indicated high false-positive rates, raising ethical concerns over human rights violations.

Why It Matters: This case serves as a cautionary tale about the dangers of deploying AI-based security measures without proper safeguards. The risk of algorithmic bias and wrongful profiling remains significant when military AI systems transition into civilian spaces.

The Current Issue with the Military AI Regulation Loophole.

Lack of Legal Oversight: Military AI is exempt from legal review requirements under Article 55 [3], allowing unrestricted development and deployment.

Transparency Deficit: Security and defense AI is exempt from transparency obligations under Article 2 [1], creating an accountability gap.

Biometric Surveillance Loophole: AI-driven biometric surveillance does not require user consent under Article 20 [5], contradicting GDPR standards.

Ethical Contradictions: Military AI exemptions violate global AI ethics guidelines, contradicting the Asilomar AI Principles and OECD AI standards.

Human Rights Risks: The unrestricted use of military AI poses threats to fundamental rights, undermining international legal protections.

4. Legal and Ethical Contradictions

4.1 The Transparency Double Standard

The Act mandates explainability and transparency for civilian AI (Article 13 [8]), yet no such requirements exist for military or law enforcement AI systems (Article 2 [1]). This lack of accountability raises concerns about unchecked AI deployments that could have far-reaching consequences on society. Without transparency obligations, AI-driven military applications could make high-stakes decisions with no public oversight, contradicting the fundamental principles of AI safety and governance. Civilian AI faces strict transparency mandates (Article 13 [8]). While Government, military, and police AI remain exempt from similar disclosure.

The Human Rights Violations are at Stake. The GDPR (General Data Protection Regulation) enforces strict AI data protection laws, yet these do not apply to military AI, raising privacy concerns.(Article 20[5]) [11] The European Convention on Human Rights (ECHR) ensures right to private life, which is undermined by unregulated biometric AI in security sectors. By exempting security AI from transparency mandates, the AI Act legitimizes mass surveillance with no legal accountability [5].

Legal & Ethical Risks. The Dangers of Unchecked Military AI in Civilian Use The AI Act does not include legal safeguards for military AI repurposing (Article 55 [3]). This regulatory gap allows high-risk AI systems to transition into domestic policing, border control, and crisis management without additional legal review or public transparency.

Failure to Align with Human Rights Regulations General Data Protection Regulation (GDPR) → Requires explicit consent for biometric AI applications, yet security AI is exempt (Article 20 [5]), undermining privacy protections; European Convention on Human Rights (ECHR) → Guarantees the right to private life and due process, yet predictive AI and biometric surveillance pose serious threats to these rights.

Strengthening the Legal Analysis:

The AI Act's military exemption relies heavily on Article 4(2) of the Treaty on European Union (TEU) [7], which establishes that "national security remains the sole responsibility of each Member State." This provision has been widely interpreted as allowing broad discretion for governments to deploy AI in defense and intelligence applications without the stringent oversight applied to civilian AI. However, this exemption creates a regulatory paradox—while the AI Act imposes strict compliance burdens on civilian developers [4], it permits unregulated state use of AI for security, surveillance, and even military applications [10].

Legal Loopholes and Contradictions. Contradiction with GDPR Protections (Article 2(1), Article 55(3)) The General Data Protection Regulation (GDPR) [11] applies strict safeguards to biometric surveillance and algorithmic decision-making that affects fundamental rights. However, the AI Act, despite being framed as a "human-centric" law, explicitly exempts military AI from these protections [6].

Article 2(1) of the AI Act states that the regulation applies to AI systems "placed on the market, put into service, or used in the Union," yet military and national security applications are excluded [1], leaving a regulatory gap where government AI can operate without the privacy and data protection safeguards enforced on private AI actors.

Article 55(3) of GDPR states that national security falls outside the jurisdiction of data protection authorities, which reinforces the lack of oversight over AI systems deployed by intelligence agencies. This creates a double standard where commercial AI is scrutinized, but state-run AI systems handling vast amounts of biometric and behavioral data are not [5].

Lack of Accountability in Military AI Development Unlike commercial AI applications, which are required to undergo risk classification, transparency reporting, and conformity assessments [9], military AI is shielded from these regulatory checks [10].

• Without mandatory legal review before repurposing military AI for civilian use, there is a serious risk of function creep—where AI developed for defense purposes gets repurposed for policing, border control, and public surveillance without democratic scrutiny [3] [15].

Precedent from EU Policy Analysis & Case Law A 2023 European Parliament study on AI governance raised concerns that the military exemption weakens the EU's commitment to fundamental rights, particularly under Article 52(1) of the Charter of Fundamental Rights [12], which requires any limitation on rights to be "necessary and proportionate."

• The European Data Protection Board (EDPB) has also warned that biometric AI in public spaces should never fall outside the scope of fundamental rights protections [5], yet the AI Act's exemptions leave a legal vacuum where military-grade AI could be quietly integrated into domestic law enforcement [3][15].

With its AI act the EU affirms seeking to lead in ethical AI governance, though it holds an AI military loophole by not requiring legal review before military AI being repurposed for civilian applications [1]; by not upholding transparency & nor impact assessments for government AI deployments [8], nor compliance with GDPR & ECHR protections in national security applications [11][12].

Without these safeguards, the AI Act risks becoming a tool for state control rather than a framework for ethical AI development.

Strengthening the Legal Analysis. The AI Act's military exemption relies heavily on Article 4(2) of the Treaty on European Union (TEU) [7], which establishes that "national security remains the sole responsibility of each Member State." This provision has been widely interpreted as allowing broad discretion for governments to deploy AI in defense and intelligence applications without the stringent oversight applied to civilian AI. However, this exemption creates a regulatory paradox—while the AI Act imposes strict compliance burdens on civilian developers [4], it permits unregulated state use of AI for security, surveillance, and even military applications [10].

4.2 A Flawed Risk-Based Framework

The regulation categorizes AI applications based on their potential societal harm (Article 6 [9]), but this framework does not account for evolving AI threats—particularly in military applications, where risk assessment is far less stringent (Article 42 [10]).

Given the rapidly changing nature of AI in warfare, the absence of oversight over AI-driven defense systems could lead to unforeseen consequences, such as autonomous AI decision-making in combat zones or civilian casualties due to algorithmic biases in military contexts. The AI Act categorizes AI risks for consumers but ignores military risks. The AI-driven autonomous decision-making in warfare raises serious questions about accountability; Algorithmic biases in combat scenarios could lead to escalation of conflict or wrongful casualties. There is an AI Ethics Breach: The Asilomar AI Principles (2017) state that AI should not be designed for autonomous warfare; The EU contradicts its own ethical stance by allowing military AI to operate without regulatory limits.

Contradictions in EU AI Policy: The Ethics Breach Despite claiming leadership in ethical AI governance, the EU AI Act permits security and military AI to operate outside transparency mandates (Article 2 [1]). This directly contradicts global AI ethics guidelines emphasizing transparency, accountability, and risk mitigation.

Asilomar AI Principles (2017) → State that AI should not be designed for autonomous warfare or policing without strict ethical review.

OECD AI Principles (2019) → Advocate for human-centered AI regulation, yet military AI remains exempt from these obligations under the AI Act.

5. Conclusion and Call for Genuine Human-Centric AI

Regulation (EU) 2024/1689 [1] presents a paradox: while it claims to be human-centric, its structural priorities suggest otherwise. By disproportionately restricting civilian AI use while allowing unchecked expansion of governmental AI, it fails to uphold its stated purpose.

This imbalance raises urgent ethical and legal concerns, particularly in the areas of transparency and accountability, human autonomy and privacy, and the dual-use risk. In terms of transparency and accountability, military and law enforcement AI remain unregulated, allowing for unmonitored surveillance and decision-making. This lack of regulation undermines public trust and raises concerns about the potential misuse of these technologies. In terms of human autonomy and privacy, the Act enables biometric AI systems to operate without consent, which undermines fundamental rights and privacy. This lack of consent raises concerns about the potential for unauthorized surveillance and the erosion of individual autonomy.

Finally, the dual-use risk is another significant concern. AI developed for military applications can be repurposed for domestic surveillance, creating unchecked risks for civil liberties. This risk is particularly concerning because it allows for the use of advanced technologies for purposes that may not be in the public interest.

To address these contradictions, this paper calls for urgent regulatory reforms. Specifically, it calls for the enforcement of transparency across all AI applications, including military and security AI. It also calls for the strengthening of user consent protections, particularly in biometric and surveillance-based AI. Finally, it calls for the closure of regulatory loopholes that allow military AI to be repurposed for domestic surveillance.

If the EU genuinely intends to lead in ethical AI governance, it must align its policies with human progress, prioritizing AI's potential to enhance relationships, autonomy, and collaboration—rather than reinforcing surveillance and militarization. If the EU genuinely wishes to lead the world in ethical AI regulation, it must address these contradictions and align its policies with fundamental human rights. Otherwise, AI will remain a tool of control, rather than an instrument of progress. If the EU intends to lead in ethical AI governance, it must close the military AI loophole. Otherwise, AI will remain a mechanism of restriction rather than a force for liberation..

Call to Action: Closing the Military AI Loophole Regulation (EU) 2024/1689 presents a paradox: while claiming to be human-centric, its structural priorities suggest otherwise. By heavily restricting civilian AI while enabling unchecked governmental AI expansion, it undermines its own purpose. This imbalance raises urgent ethical and legal concerns—particularly regarding transparency, accountability, and individual autonomy.

To align AI regulation with genuine human progress, urgent reforms are needed. The EU must:

•Enforce mandatory legal review before repurposing military AI for civilian use

•Implement strict transparency and accountability measures for AI in law enforcement

•Ensure full compliance with GDPR and ECHR protections for biometric surveillance

Without these safeguards, AI will continue to serve state power over individual rights, eroding civil liberties rather than promoting human-centric innovation. If the EU truly aims to lead in ethical AI governance, it must close these regulatory gaps—ensuring AI serves humanity, not just governmental control.

Disclosure of Interests. The author has signed the Asilomar AI Principles, endorsing the ethical development and governance of artificial intelligence in alignment with transparency, accountability, and human-centric values. This declaration informs the analytical perspective of this paper, which critically evaluates Regulation (EU) 2024/1689 against internationally recognized AI ethics frameworks, including Asilomar and the OECD AI Principles.

The author declares no financial or institutional conflicts of interest. The views expressed herein are independent and solely those of the author, reflecting a commitment to responsible AI research and governance.

References

1. Regulation (EU) 2024/1689, Official Journal of the European Union: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
2. AI Act - High-Risk AI Categories, EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0694
3. AI in Law Enforcement and Surveillance, EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0038
4. AI Restrictions for Private Sector, EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0041
5. Biometric AI Compliance, EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0013
6. Recital 24 of AI Act, EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
7. Treaty on European Union (TEU), EUR-Lex: https://eur-lex.europa.eu/eli/treaty/teu_2012/art_4/oj/eng
8. Transparency Requirements for AI, EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
9. Risk Classification in AI Act, EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
10. AI in Military Applications, EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
11. GDPR Official Text: https://gdpr-info.eu/
12 ECHR: official European Convention of Human Rights : https://www.echr.coe.int/documents/d/echr/convention_eng
13. Asilomar AI Principles: https://futureoflife.org/open-letter/ai-principles/
14. OECD AI Principles: https://oecd.ai/en/ai-principles
15. EU iBorderCtrl Project Report: https://cordis.europa.eu/project/id/700626/reporting; https://www.patrick-breyer.de/en/posts/iborderctrl; https://www.iborderctrl.eu/iborderctrl-project-the-quest-of-expediting-border-crossing-processes.html