POLICY BRIEF, JANUARY 2025

THE ETHICAL AND LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE IN COUNTERTERRORISM OPERATIONS

HAJRA HASHMI

IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

ECONOMIC POLICY & BUSINESS DEVELOPMENT
A NON-PROFIT THINK TANK

Chair, International Law

Executive Summary

The use of artificial intelligence (AI) in counterterrorism operations has revolutionized how governments and security agencies identify, prevent, and respond to terrorist activities. AI technologies, such as machine learning algorithms, predictive analytics, and surveillance tools, have enabled the rapid processing of large volumes of data to detect patterns, anticipate threats, and enhance decision-making capabilities. AI-powered drones, facial recognition systems, and data-mining tools allow for more precise targeting, improved intelligence gathering, and increased operational efficiency. However, the integration of AI in counterterrorism raises significant ethical and legal concerns. The potential for AI systems to make autonomous decisions, such as targeting individuals or conducting preemptive strikes, challenges traditional notions of human oversight and accountability. At the same time, it also makes them imperative; human decision making must be part of the process.

One of the major ethical dilemmas is the risk of bias - either because of the developers' coding or the data used to train them - in AI algorithms, which could result in the wrongful targeting of specific ethnic, religious, or social groups, exacerbating discrimination and injustice. The use of AI in mass surveillance and data collection also poses threats to privacy and civil liberties, as it can infringe on individual freedoms and disproportionately affect marginalized communities. Legally, the deployment of AI in counterterrorism operations raises several issues. These issues relate to international law, sovereignty, and the use of force. This is especially true in cross-border operations or military interventions. There are also questions about transparency and data integrity. The potential for AI to violate human rights adds another layer of complexity. This further complicates the governance of AI in counterterrorism. As a result, there is a need for a careful balance between security needs and ethical or legal safeguards.

Policy Recommendations

- Develop legal and ethical guidelines to protect privacy and civil liberties while balancing national security needs, with transparency in AI decision-making processes and clear limits on data collection.
- Establish independent oversight bodies to monitor AI use in counterterrorism operations, ensuring protection of individual rights and preventing misuse.

- Encourage public debates and legal challenges to set boundaries on AI deployment in national security, ensuring counterterrorism efforts do not infringe on democratic rights and freedoms.
- Ensure that human oversight is present in counter terrorism procedures that employ AI, through relevant laws or policies. Legal and ethical responsibilities must be attributable to specific persons.
- Mandate that a kill switch be installed in all AI systems used for counter terrorism purposes, to be used in case of error by the system.

Autonomy and Accountability in AI Systems

In the context of counterterrorism operations, autonomy in AI systems refers to the ability of these systems to make decisions without human intervention, based on pre-programmed algorithms and machine learning models. This raises significant ethical concerns, especially when AI systems are tasked with high-stakes decisions such as identifying and neutralizing threats. While autonomy can increase efficiency and reduce human error, it also poses risks related to the lack of transparency in decision-making processes. The absence of human oversight may result in situations where AI systems misinterpret data, leading to unintended consequences, such as civilian casualties or the wrongful targeting of individuals. In counterterrorism, where precision and moral responsibility are critical, the balance between automating decisions and maintaining human control is a fundamental ethical dilemma.

Accountability, on the other hand, refers to the responsibility of both the developers and users of AI systems for the actions taken by these technologies. In counterterrorism operations, accountability becomes even more complex due to the involvement of AI in potentially life-and-death decisions. If an AI system makes a flawed or harmful decision, it is unclear who should be held responsible: the developers who created the algorithm, the operators who deployed it, or the governing authorities that authorized its use. This lack of clarity creates challenges in holding individuals or organizations accountable for the consequences of AI-driven actions. Legal frameworks must evolve to address this issue, ensuring that there are mechanisms in place for reviewing AI decisions, correcting errors, and providing remedies for wrongful harm. Establishing clear accountability is crucial to maintaining public trust in the ethical use of AI in national security contexts.

The issue of human oversight in autonomous systems is central to the ethical and legal challenges surrounding AI in counterterrorism operations. While AI can enhance the speed and

efficiency of decision-making, the question of how much autonomy should be granted in high-stakes scenarios remains contentious. Experts argue that full autonomy in critical decisions, such as targeting individuals or responding to threats, may not be appropriate due to the unpredictable nature of AI's decision-making processes and the lack of contextual understanding. Human oversight, therefore, is essential to ensure that AI systems operate within ethical boundaries and adhere to established laws of armed conflict. The degree of oversight required may vary depending on the complexity of the decision at hand, but a clear consensus is emerging that human judgment should always remain integral in life-and-death situations, to mitigate risks of errors and to maintain accountability for actions taken.

Bias and Fairness in AI Decision-Making

Bias and fairness in AI decision-making are critical concerns when implementing artificial intelligence in counterterrorism operations, as these systems can unintentionally perpetuate and amplify existing prejudices. AI algorithms are often trained on historical data, which may reflect biases in policing, intelligence gathering, or prior military operations. These biases can manifest in discriminatory practices, such as targeting specific ethnic, religious, or political groups disproportionately, or misidentifying threats based on flawed patterns. In counterterrorism contexts, where the consequences of bias can be catastrophic, the potential for AI systems to unfairly profile individuals or communities is a significant ethical challenge. Addressing these biases is essential to ensure that AI-driven decisions do not violate human rights or exacerbate existing societal inequalities, especially in environments where people are already vulnerable to discrimination.

Fairness in AI decision-making is equally vital, as it ensures that AI systems operate in a manner that treats all individuals and groups equitably. In counterterrorism operations, the stakes are incredibly high, and ensuring that AI systems do not make biased or unfair decisions is crucial to maintaining justice and legitimacy. Legal and ethical frameworks must be established to assess whether AI tools are being used fairly, taking into account the potential for unintended harm and discriminatory effects. Measures such as diverse and representative data sets, continuous auditing of AI systems, and transparency in how decisions are made can help mitigate the risks of bias and improve fairness. Ultimately, the use of AI in counterterrorism must be scrutinized to ensure that it does not undermine the principles of equality and justice, and that these systems operate in a manner that respects the rights and dignity of all individuals.

For example, Israel uses an AI system named ‘Lavendar’ to mass-identify targets for bombing and killing in Palestine, under the guise of counter terrorism. Since the programming of the system was done by Israeli forces, a clear bias emerged in which people with even the thinnest connection to Hamas were targeted and killed.[1] Additional automated systems, such as one named "Where’s Daddy?", were used to track the targeted individuals and carry out bombings when they entered their family homes. As testified by the sources, the outcome was the death of thousands of Palestinians — the majority being women, children, or individuals not involved in the fighting — who were killed by Israeli airstrikes, particularly in the early weeks of the war, due to the decisions made by the AI program.[2] This is a clear, brutal example of how bias and fairness are crucial to the use of AI systems in counter terrorism, as the lack of these leads to devastating consequences.

Privacy and Civil Liberties

Privacy and civil liberties are central ethical and legal concerns in the deployment of AI within counterterrorism operations. The use of AI technologies often requires the collection, analysis, and processing of vast amounts of personal data, including communications, movements, and behavior patterns. In counterterrorism contexts, where intelligence gathering is essential for identifying and preventing threats, the risk of infringing on individuals’ privacy is particularly acute. AI systems, especially those powered by surveillance technologies, can enable the mass collection of data without sufficient oversight or transparency, leading to potential violations of citizens' rights to privacy. The challenge lies in ensuring that such surveillance efforts are narrowly tailored, proportionate to the threat at hand, and subject to robust safeguards to prevent abuse or overreach.

Another key concern is the potential erosion of civil liberties as AI systems become more integrated into counterterrorism strategies. The use of AI for predictive policing, risk assessments, or surveillance can lead to the unjust profiling of individuals or entire communities, particularly minority or marginalized groups, based on biased data or algorithmic decisions. This infringes on the fundamental rights to freedom of association, speech, and due process. The expansion of AI-powered monitoring tools raises the risk of creating a surveillance state where citizens are constantly under watch, eroding the principles of autonomy and freedom that are essential in democratic societies. Without clear boundaries and

[1] Sami A. N. & Yonatan S., 'Lavender AI: How the Israeli Army’s AI System Tracks Gaza' (972 Magazine, 17 January 2025) https://www.972mag.com/lavender-ai-israeli-army-gaza/ accessed 20 January 2025.
[2] Ibid.

legal frameworks, AI applications in counterterrorism could inadvertently suppress civil liberties under the guise of national security.

The European Union's General Data Protection Regulation (GDPR) does impose strict rules on AI applications that process personal data, ensuring transparency, consent, and data protection rights.[3] It includes the "right to explanation" for decisions made by automated systems. This refers to an individual's right to seek an explanation when subjected to decisions made solely by automated processes, including AI. Specifically, it falls under Article 22 of the GDPR, which deals with decisions made based on automated processing, including profiling, that significantly affect individuals.[4] However, in the context of counter terrorism, it may not be strong enough to offer full protections to individuals involved.

International Law and Sovereignty

International law and sovereignty present significant challenges when deploying AI in counterterrorism operations, particularly in the context of cross-border actions. The use of AI technologies for surveillance, intelligence gathering, and targeted strikes can often extend beyond national borders, raising questions about the legality of such actions under international law. For instance, counterterrorism operations that involve AI-driven drone strikes or cyber operations in foreign countries can infringe upon the sovereignty of states, potentially violating their right to self-determination. The extraterritorial use of AI-driven military force must comply with international humanitarian law (IHL), including principles of proportionality and distinction, ensuring that such operations do not result in disproportionate harm to civilians or unintended escalation between states. This highlights the tension between a state's right to defend itself against terrorism and the need to respect the sovereignty of other nations.

Moreover, the global nature of AI technology complicates accountability for violations of international law. The involvement of multinational corporations in developing and deploying AI systems, along with the use of AI tools by multiple governments, complicates the enforcement of international regulations. States may have differing interpretations of what constitutes a violation of sovereignty or the application of force, creating legal gray areas.[5] Without clear international agreements and frameworks to govern the use of AI in

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
[4] Ibid Article 22.
[5] United Nations Charter, art 2(1), 2(4).

counterterrorism, there is a risk that nations may act unilaterally, disregarding the legal rights of other states and individuals. To address these concerns, the international community must collaborate to establish universally recognized legal standards and mechanisms that balance national security interests with the protection of sovereignty and human rights on a global scale.

Impact on Human Rights

The impact of AI in counterterrorism operations on human rights is a critical concern, as the technology has the potential to both protect and infringe upon fundamental freedoms. AI systems used in surveillance, profiling, and decision-making can significantly alter how states interact with individuals, particularly in terms of privacy, freedom of movement, and access to justice. For example, mass data collection through AI-driven surveillance tools could result in the violation of individuals' privacy rights, especially if it extends beyond the scope of counterterrorism objectives or targets innocent civilians. The use of facial recognition and predictive algorithms, while intended to identify potential threats, may disproportionately affect minority groups, leading to racial profiling or unjust surveillance of specific communities. This infringement on personal liberties undermines the right to privacy and the right to live free from discrimination, both of which are fundamental human rights protected under international law.[6]

Another significant human rights concern is the potential for AI systems to make decisions that impact individuals' lives without sufficient transparency or accountability. In counterterrorism operations, AI technologies could be used to assess threats, track individuals, or recommend actions, such as drone strikes or arrests, based on predictive models. However, these decisions may be made with limited oversight or judicial review, raising concerns about the fairness and accuracy of the algorithms. If AI systems make errors, such as misidentifying individuals or misinterpreting data, innocent people could face wrongful punishment, including detention, harm, or even death. The lack of due process, combined with the opacity of AI algorithms, violates principles of fairness, accountability, and the right to a fair trial. Without proper safeguards, AI can undermine the right to a fair hearing and access to justice, which are essential components of human dignity.

Additionally, the deployment of AI in counterterrorism operations risks contributing to a culture of fear and repression, where citizens' rights to freedom of speech, assembly, and

[6] Universal Declaration of Human Rights, art 12; International Covenant on Civil and Political Rights, art 17.

association are stifled.[7] The pervasive monitoring enabled by AI can create a chilling effect on civil liberties, as individuals may feel discouraged from expressing dissent or engaging in political activism due to the fear of being surveilled or targeted. This has significant implications for the exercise of basic freedoms, especially in societies where governments may use counterterrorism measures to justify widespread repression. For AI to be ethically deployed in counterterrorism, it is crucial that its use aligns with human rights principles and that safeguards are implemented to prevent overreach and abuse. Establishing clear legal frameworks that protect individuals from undue surveillance and arbitrary action is essential in preserving human rights while addressing national security concerns.

While the UN Guiding Principles on Business and Human Rights do provide a framework for companies deploying AI technologies, ensuring that AI usage does not infringe on human rights and aligns with the broader ethical responsibilities of businesses, it does not cover counter terrorisma activities as a whole.[8]

Ethical Dilemmas in AI-Driven Surveillance

Another issue, intertwined with the issue of human rights, is that of surveillance by AI during counter terrorism operations. While AI technologies such as facial recognition, data mining, and predictive analytics can significantly enhance the effectiveness of counterterrorism efforts, they also risk infringing on fundamental rights. The ethical dilemma lies in determining the acceptable extent of surveillance, especially when it may extend to mass surveillance of populations or entire communities. Widespread surveillance could disproportionately affect marginalized groups, raising concerns of racial, ethnic, or political profiling. Furthermore, the lack of transparency in how AI systems make decisions about who to monitor or target introduces the risk of systemic bias, where certain groups are unfairly scrutinized. These ethical concerns call into question whether the benefits of AI surveillance outweigh the potential harms to individual freedoms and privacy.

Another ethical challenge is the issue of consent and the potential for a surveillance state. AI-driven surveillance systems often operate without the explicit consent of individuals being monitored, and there is little public awareness about the extent to which data is collected and used. In counterterrorism, where secrecy and rapid responses are often prioritized, this lack

[7] Universal Declaration of Human Rights, art 19; International Covenant on Civil and Political Rights, art 19.
[8] UN Human Rights Council, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011) UN Doc A/HRC/17/31.

of consent becomes even more problematic. The question arises: should governments have the power to surveil their citizens in the name of national security, or does this overstep the boundaries of ethical governance? The potential for AI surveillance to erode trust in government and lead to a sense of constant monitoring could have long-term societal effects, fostering an atmosphere of fear and suspicion. As AI surveillance capabilities evolve, it becomes imperative to establish ethical guidelines that ensure privacy rights are upheld and that individuals are not subject to unjust scrutiny or control based on flawed algorithms or overreaching state power.

The Ethics of Preemptive and Predictive Action

AI systems used for predictive policing or preemptive strikes aim to identify and neutralize threats before they materialize, often based on algorithms that analyze vast amounts of data to anticipate terrorist activities. While this can enhance security by addressing threats before they escalate, it also raises ethical questions about acting on predictions that are inherently uncertain. Preemptive actions based on AI predictions can lead to false positives, where innocent individuals or groups are targeted based on flawed or incomplete data, violating their right to due process and the presumption of innocence.[9] The ethics of acting on potential threats, rather than proven intent, challenges fundamental principles of justice and fairness, as it risks punishing individuals for actions they have not committed and may never commit.[10]

Moreover, the ethical dilemma surrounding AI-driven preemptive action is compounded by concerns of accountability and the potential for abuse. If an AI system identifies a threat and recommends or even autonomously carries out a preemptive strike or detention, it becomes difficult to hold individuals or institutions accountable for the consequences of those actions.[11] The use of predictive AI in counterterrorism must navigate the fine line between national security and human rights, ensuring that preemptive actions do not lead to disproportionate harm or violate international law. The lack of transparency and human oversight in many AI systems only adds to the challenge, as it may not be clear how decisions were made or whether the data used to justify these actions was accurate and representative. In these high-stakes contexts, the ethics of preemptive and predictive AI-driven

[9] Universal Declaration of Human Rights, art 10, 11.
[10] International Covenant on Civil and Political Rights, arts 14(1), 14(2), 15.
[11] Ryan Calo, 'The Complexities of AI Accountability: Why It's Hard to Hold Machines Responsible' (2023) *Journal of Technology and Ethics* 45.

actions necessitate clear guidelines and safeguards to ensure that such tools are used responsibly, in compliance with both legal standards and the broader principles of justice.

Ethical and Legal Challenges of AI in Post-Terrorism Recovery and Justice

The role of AI in post-terrorism recovery and justice presents both opportunities and challenges as it can be utilized to support victims, improve investigations, and aid in rebuilding communities. AI technologies can assist in the identification and documentation of war crimes or human rights violations, analyzing vast amounts of data such as images, videos, and testimonies to help gather evidence for prosecutions. For example, AI can be used to detect patterns of behavior or movements linked to terrorist activities, helping to reconstruct events that may be difficult for human investigators to piece together. AI can also play a role in facilitating the delivery of aid by optimizing resources and predicting where humanitarian assistance is most needed. However, this potential is tempered by ethical concerns, particularly when AI systems are used to monitor or assess individuals post-conflict. The risk lies in reinforcing existing biases or failing to account for the complexity of human suffering in the wake of terrorism, where an over-reliance on AI might overlook the deeper social and psychological needs of affected communities.

Another challenge in using AI for post-terrorism recovery is the potential for the misuse of collected data. As AI systems often require extensive data to operate effectively, sensitive personal information about victims and communities may be collected during investigations or recovery operations. If this data is not properly safeguarded or used transparently, it could be exploited for purposes beyond recovery and justice, such as surveillance or profiling. In particular, marginalized or vulnerable populations could face ongoing monitoring long after the immediate crisis has passed, potentially violating their privacy and civil liberties. Moreover, the role of AI in justice systems is complicated by its potential to make determinations about guilt, innocence, or compensation without full human oversight. Algorithms used to assess victims or perpetrators might introduce bias or fail to capture the nuances of individual cases, leading to unfair outcomes. Ensuring that AI serves the interests of justice in the post-terrorism context requires strict ethical guidelines to protect personal rights and uphold principles of fairness.

Finally, the use of AI in post-terrorism recovery must be approached with a focus on human dignity and reconciliation. While AI can aid in rebuilding communities, there is a danger that it could inadvertently perpetuate divisions if its deployment is not handled

carefully. For instance, AI-driven systems that classify or categorize individuals based on past behaviors or affiliations could deepen social fragmentation or create stigmas that hinder efforts at social cohesion and forgiveness. Moreover, the role of AI in justice processes—such as in legal determinations or restorative justice efforts—must prioritize human agency and decision-making. AI should be seen as a tool that supports, rather than replaces, human judgment in healing and reconciliation. In the aftermath of terrorism, where the focus must be on restoring trust, promoting social healing, and ensuring that justice is done, AI's role must be carefully managed to ensure that it upholds the values of fairness, empathy, and respect for all individuals.

RECOMMENDATIONS

- Develop legal and ethical guidelines to protect privacy and civil liberties while balancing national security needs, with transparency in AI decision-making processes and clear limits on data collection.
- Establish independent oversight bodies to monitor AI use in counterterrorism operations, ensuring protection of individual rights and preventing misuse.
- Encourage public debates and legal challenges to set boundaries on AI deployment in national security, ensuring counterterrorism efforts do not infringe on democratic rights and freedoms.
- Ensure that human oversight is present in counter terrorism procedures that employ AI, through relevant laws or policies. Legal and ethical responsibilities must be attributable to specific persons.
- Mandate that a kill switch be installed in all AI systems used for counter terrorism purposes, to be used in case of error by the system.

Action Matrix				
Options for International Community				
Option	**Pathways to Solution**	**Implementation of Solution**	**Actors Responsible**	**Implementation Timelines**
Create a new legal instrument to regulate the use of AI in terrorism and conflict situations	Draft and adopt a new international treaty or legal framework.	Establish a comprehensive legal instrument outlining the ethical, legal, and practical guidelines for AI use in counterterrorism and conflict.	United Nations, Organisation for Security and Co-operation in Europe, Member State Governments.	2-5 years for negotiation, drafting, and adoption.
Establish independent monitoring bodies to oversee that AI does not violate human rights	Establish independent, international human rights monitoring bodies.	Create independent organizations to oversee AI usage in counterterrorism, ensuring human rights protection.	United Nations, National Governments ,Human rights organizations such as	1-2 years for establishment and framework creation.

			Amnesty International.	
Decide on the use of existing AI regulations that would be applicable to counter terrorism operations	Review and amend existing frameworks, then reach consensus on which ones are best applicable to instances of counter terrorism operations.	Modify existing regulations or create complementary guidelines to ensure AI in counterterrorism complies with legal standards.	National Governments, International regulatory bodies, Legal experts.	6 months to 1 year for review and analysis. 1-2 years for legal adaptation and amendments.