Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 9 (September) (2025)

Artificial Intelligence and the Right to Privacy: A Human Rights Dilemma in the Age of Surveillance

Muhammad Raees Malik
Lecturer Laws Rashid Latif Khan University Lahore.

ABSTRACT
The rapid proliferation of artificial intelligence (AI) technologies, particularly those deployed for surveillance purposes, present profound challenges for the fundamental human right to privacy. This research paper provides a comprehensive examination of the intersection between AI-driven surveillance and privacy rights exploring the evolving global legal frameworks with a focus on Pakistan's legislation. By critically analyzing international and regional laws alongside emerging AL applications, this study highlights the dilemmas faced by policymakers, legal practitioners and society at large. It underscores the urgent need for robust legal mechanisms and ethical considerations to safeguard privacy without undermining technological innovation and public security.

Key Words: Artificial Intelligence, Privacy, Human Rights, Surveillance, UDHR, ICCPR, Legislation, GDPR, Pakistan, Data Protection, Ethical Framework.

Introduction:
The integration of Artificial Intelligence in surveillance systems has transformed the landscape of privacy rights globally. AI technologies such as facial recognition, predictive policing algorithms and biometric data processing enable unprecedented levels of data collection and analysis, often occurring covertly. As these tools advance, they challenge traditional paradigms of privacy and pose risks of mass surveillance raising urgent human rights concerns. Governments and private enterprises increasingly deploy AI surveillance in pursuit of security and economic goals; however, this trend often conflicts with individuals' fundamental right to privacy, autonomy and freedom from discrimination. The tension between leveraging AI for societal benefit and protecting privacy constitutes a critical dilemma at the heart of contemporary human rights discourse **(H.WH. Chan, N.P.K. Lo).**
This paper seeks to delineate the complexity of this dilemma by examining current international legal frameworks, regional legislation with particular emphasis on Pakistan, and the ethical challenges inherent in AI surveillance. It explores technological advancements, legal responses and policy recommendations to reconcile AI innovation with respect for privacy and human dignity.

Literature Review and Theoretical Framework:
AI and Privacy: Technological and Ethical Challenges.
AI-powered surveillance technologies have transformed data collection, enabling continuous monitoring and predictive analytics that expose intimate details of individuals' lives. Advance systems such as facial recognition, AI-driven drones and smart sensors facilitate pervasive surveillance eco systems that undermine traditional notions of consent and privacy. These technologies often operate in opaque environments marked by limited transparency, accountability and human oversight, exacerbating risks marked by limited social control, especially against marginalized groups **(H.W.H. Chan and N.P.K. Lo).** The normalization of such surveillance threatens social norms related to

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 9 (September) (2025)

privacy, freedom of expression and assembly. **(G. Gabrielli).**
Ethically, AL surveillance introduces dilemmas that extend beyond technological limitations, raising questions about fairness, transparency and the privatization of social control. Current framework often struggles to ensure informed consent and adequate safeguards, underscoring the need for privacy by design approaches, algorithmic transparency and human rights centered governance mechanisms (H.W.H. Chan and N.P.K. Lo), (M. Milossi).

Legal Challenges in Governing AL Surveillance

The fast-evolving capabilities of AI outpace the development of legal frameworks worldwide, resulting in regulatory gaps and contentious debates about the adequacy of existing laws. There is consensus among scholars that AI introduces new challenges to human rights protection especially concerning algorithmic transparency, bias, lack of accountability and data privacy (**R. Rodrigues).** International human rights law has yet to fully adapt to AI-Driven surveillance, requiring dynamic legal and ethical frameworks responsive to emerging risks (**F. Roumate).**
The European Union's General Data Protection Regulation (GDPR) stands as prominent example of a robust legal structure design to address data privacy and AI ethics, emphasizing consent, transparency and data protection by design. Nonetheless, critiques note the even GDPR faces challenges in fully encompassing the nuances of AI surveillance technologies and their societal impacts **(M. Milossi), (D. Almeida, K. Shmarko, E. LomasI).** Other jurisdictions, including Pakistan, grapple with underdeveloped frameworks lacking stringent date protection laws and comprehensive AI governance strategies, increasing vulnerability to privacy infringements (**B. Ehimuan, O. O. Chimezie, O. V. Akagha, O. Reis, B. B. Oguejiofor).**

Methodology

This research employs a doctrinal legal analysis supported by a multidisciplinary review of AL surveillance technologies, ethical concerns and legislative frameworks. It systematically compares global legislation, focusing on GDPR and emergent AI regulatory proposals with Pakistan's current legal environment on data privacy and surveillance. The paper incorporates critical evaluative synthesis, identifying strengths, weaknesses and gaps, while providing policy recommendations rooted in human rights principles.

Global Legislative Frameworks Addressing AI Surveillance and Privacy

European Union: General Data Protection Regulation and the Artificial Intelligence Act.

The EU's GDPR constitutes the most comprehensive framework for data protection, establishing principles such as lawfulness, fairness, transparency, data minimization and purpose limitation to protect induviduals' privacy rights. GDPR integrates robust obligations for data controllers and processors, including data subject rights to access, ensure and objection which are pivotal in curbing AI's potential misuse in surveillance **(M. Milossi).** The regulation also foster "privacy by design" and "privacy by default" concepts, mandating that AI systems incorporate privacy safeguards from inception.
Recognizing that AI's distinct challenges, the European Commission proposes that Artificial Intelligence Act to create tailored rules emphasizing risk-based approaches. This includes prohibiting certain high-risk AI uses such as biometric mass surveillance unless stringent safeguards apply and enhancing transparency and third-party conformity

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 9 (September) (2025)

assessments **(I. Barkne).** Despite these advances, critiques highlight loopholes concerning emotional recognition technologies and exceptions that may dilute protections, mandating stronger prohibitions and accountability mechanisms (**I. Barkne).**

United States: Fragmented Privacy Laws and Surveillance Practices

Unlike the EU the United States lacks a unified federal data privacy law comparable to GDPR. Instead, it has a patchwork of sector-specific status such as the California Consumer Privacy Act (CCPA), which attempts to enhance consumer rights but does not fully regulate AI surveillance (**B. Ehimuan, O. O. Chimezie, O. V. Akagha, O. Reis, B. B. Oguejiofor).** The enforcement of privacy rights is uneven, and AI surveillance technologies deployed by law enforcement often operate with limited oversight. This fragmented governance increases risks of unregulated mass surveillance and abuses **(D. Almeida, K. Shmarko, E. Lomas).**

Emerging Legal Developments and Challenges in Asis and Other Regions

Asian countries demonstrate diverse approaches, with some adopting strong data protection laws and ither relying on reactive regulatory updates. The rapid integration of AI into public administration and policing often outpaces legal safeguards, engendering concerns about human rights impacts and privacy violations **(O. Reis, N. E. Eneh, B. Ehimuan, A. Anyanwu, T. Olorunsogo, T. O. Abrahams).** International cooperation and harmonization remain limited, complicating effective enforcement and global data flow protections.

Privacy and AI Surveillance in Pakistan: Current Status and Legislative Gaps

Pakistan's legal environment regards AI and privacy rights remains embryonic, marked by fragmented laws and limited institutional capacity. The principal legislative instrument addressing data protection is the Prevention of Electronic Crimes Act (PECA) 2016, which criminalizes cyber offences but lacks comprehensive safeguards tailored for AI technologies and mass surveillance **(B. Ehiuman, O. O. Chimezie, O. V. Akagha, O. Reis, B. B. Oguejiofor).** There is notable absence of a dedicated data protection law aligned with international standards like GDPR.

Further, the legislative framework does not adequately address consent, transparency, and accountability in AI applications, exposing citizens to invasive surveillance practices that could infringe upon fundamental rights. This gap renders vulnerable the right to privacy, freedom of expression and protection against discrimination, especially considering the pervasive use of biometric and AI-enabled surveillance in law enforcement and border security (**A. A. Badhan, M. N. Hasnain, M. H. Rahman, I. Chowdhury, M. A. Sayem).** Scholars argues for Pakistan to adopt data protection legislation incorporating principles of privacy by design, independent oversight bodies, transparency obligations and clear remedies for rights violations **(S. S. Daubassova, G. T. Alaeva, K. A Dzhumabayeva).**

Human Rights Considerations in the Age of AI Surveillance

The right to privacy is enshrined in universal human instruments, including Universal Decleration of Human Rights (UDHR) and the International Convention on Civil and Political Rights (ICCPR). AI surveillance raises thorny issues about upholding these rights in practice. The normalization of AI-based surveillance risks eroding domestic freedoms, as continuous monitoring constrains freedom of assembly and expression (**G. Gabrielli).** The covert and automated nature of AI surveillance challenges individuals'

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 9 (September) (2025)

agency and raised the specter of digital panopticons, where social control is privatized and unaccountable **(E. Kosta).**

Moreover, discriminatory biases embedded in AI systems exacerbate inequalities and marginalize vulnerable groups. The opacity of algorithmic decision-making compounds these problems, as affected individuals find limited avenues for redress or contestation **(R. Rodrigues).** The necessity of adopting human rights-centered AI governance, including meaningful transparency, privacy-by-design, and human oversight, has emerged as a critical policy imperative to safeguard individual dignity and domestic values (**H. E. H. Chan, N. P. K. Lo).**

Case Studies: AI Surveillance in Public Security and Border Control.

AI-driven surveillance plays a pivotal role in enhancing security measures, including border control and crime prevention. In the United States, advanced surveillance ecosystems integrated AI, UAVs, and sensor networks aim to mitigate unauthorized border entries. While technology enhances detection capabilities and situational awareness about privacy infringement, racial profiling, and ethical oversight complicate these deployments **(I. A. Badhan, M. N. Hasnain, M. H. Rahman, I. Chowdhury, M. A. Sayem).** These concerns highlight the need for the robust regulatory oversight that balances security and human rights, involving collaboration among government agencies, technology firms, and civil society.

Similarly, Kazakhstan's adoption of AI in criminal surveillance reveals legal and ethical challenges, emphasizing a pressing need for a independent oversight and data protection framework to balance public safety with civil liberties (**S. S. Daubassova, G. T. Alaeva, K. A. Dzhumabayeva).**

Policy Recommendations:

Development of comprehensive Data Protection Laws: Pakistan should enact dedicated legislation aligned with international standards such as GDPR, ensuring data legislation aligned with international standards such as GDPR, ensuring data subject rights, consent requirement and mechanisms for contestability.

Privacy-by-Design and Algorithmic Transparency: AI systems must embed privacy considerations from their design phase and disclose intelligible information concerning data processing and automated decision-making.

Independent Oversight Mechanisms: Regulatory bodies with strong mandates and technical expertise are essential to monitor AI deployments, ensure compliance and address rights violations.

Multi-Stakeholder Collaboration: Policymakers, technologists, legal experts and civil society organizations should engage in ongoing dialogue to adapt frameworks dynamically to evolving technological landscapes.

Ethical AI Governance: Promote international cooperation to develop ethical standards and legal norms that prioritize human dignity, non-discrimination and democratic freedoms **(H. W. H. Chan, N. P. K. Lo) and (B. C. Stahl, R. Rodrigues, N. Santiago, K. Macnish).**

Conclusion:

Artificial intelligence fundamentally challenges the traditional understanding and protection of privacy in the contemporary digital age. The deployment of AI in surveillance exacerbates risks of Privacy violations, discrimination and erosion of

ISSN Online: 3007-3154
ISSN Print: 3007-3146

democratic freedoms. While jurisdictions like European Union have made considered strides with GDPR and the AI act, many countries, including Pakistan, lag in comprehensive legislation in institutional framework. Bridging this gap requires harmonizing legal protections with ethical AI governance, creating accountable, transparent and harmonizing legal protections with ethical AI governance, creating accountable, transparent and human rights-compliant AI surveillance ecosystems globally. Further research must explore the interplay between cultural, legal and technological dimensions to develop universally applicable, yet context-sensitive policies to protect privacy rights effectively.

References

H. W. H. Chan, N. P. K. Lo, "A Study on Human Rights Impact with the Advancement of Artificial Intelligence," Journal of Posthumanism, 2025. https://doi.org/10.63332/joph.v5i2.490AI surveillance's human rights impact, emphasizing privacy erosion and societal norms

G. Gabrielli, "The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights," European Journal of Risk Regulation, 2025. https://doi.org/10.1017/err.2025.26

M. Milossi, E. Alexandropoulou-Egyptiadou, K. E. Psannis, "AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach," Institute of Electrical and Electronics Engineers, 2021. https://doi.org/10.1109/access.2021.3072782.

R. Rodrigues, "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities," Elsevier BV, 2020. https://doi.org/10.1016/j.jrt.2020.100005

F. Roumate, "Artificial Intelligence, Ethics and International Human Rights Law," The International Review of Information Ethics, 2021. https://doi.org/10.29173/irie422

D. Almeida, K. Shmarko, E. Lomas, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks," Springer Nature, 2021. https://doi.org/10.1007/s43681-021-00077-w.

B. Ehimuan, O. O. Chimezie, O. V. Akagha, O. Reis, B. B. Oguejiofor, "Global data privacy laws: A critical review of technology"s impact on user rights," GSC Online Press, 2024. https://doi.org/10.30574/wjarr.2024.21.2.0369.

I. Barkne, "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance1," IOS Press, 2022. https://doi.org/10.3233/ip-211524.

O. Reis, N. E. Eneh, B. Ehimuan, A. Anyanwu, T. Olorunsogo, T. O. Abrahams, "PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT," Fair East Publishers, 2024. https://doi.org/10.51594/ijarss.v6i1.733.

I. A. Badhan, M. N. Hasnain, M. H. Rahman, I. Chowdhury, M. A. Sayem, "Strategic Deployment of Advance Surveillance Ecosystems: An Analytical Study on Mitigating Unauthorized U.S. Border Entry," None, 2024. https://doi.org/10.63544/ijss.v3i4.105

S. S. Daubassova, G. T. Alaeva, K. A. Dzhumabayeva, "AI and criminal surveillance in Kazakhstan," None, 2025. https://doi.org/10.46914/2959-4197-2024-1-4-19-29.

E. Kosta, "Algorithmic state surveillance: Challenging the notion of agency in human rights," Wiley, 2020. https://doi.org/10.1111/rego.12331.

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 9 (September) (2025)

B. C. Stahl, R. Rodrigues, N. Santiago, K. Macnish, "A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values," Elsevier BV, 2022. https://doi.org/10.1016/j.clsr.2022.105661