



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Artificial Intelligence on Civil Liberties and Privacy Rights

Introduction:

The realm of artificial intelligence has rapidly evolved from a realm of science fiction to an integral part of our daily lives. With advancements in technology, AI now plays a crucial role in shaping our digital landscape. As it continues to grow in influence, concerns about its impact on human rights and privacy have become more pronounced. Society's increasing adoption of AI surveillance tools raises questions about personal freedoms. From facial recognition to predictive analytics, the wide range of data-gathering methods poses a threat to privacy. As AI technology advances, the distinction between preventing crime and violating privacy becomes less clear, underscoring the need for strong legal protections. Despite its benefits, AI's heavy reliance on data poses risks to individual privacy and must be carefully managed.¹ Recent strides in AI technologies have raised apprehensions about their potential misuse to inflict harm. Visualizations accompanying these concerns underscore that AI is already influencing the enjoyment of a comprehensive array of human rights, sometimes in paradoxical ways.²

Violation of public safety and individual rights:

AI-driven surveillance systems operate through gathering vast amounts of data from a variety of sources like cameras, sensors, and social media. Complex algorithms then analyze this data to spot patterns, uncover suspicious activities, and forecast potential threats. While these systems are effective in preventing crimes and ensuring public safety, there are concerns about their intrusive nature, leading to issues of privacy invasion, discrimination, and misuse. One major concern is the loss of privacy, as these systems can collect detailed information about individuals, including their movements, habits, and emotions. This information, stored and analyzed indefinitely, can be used for targeted advertising, political profiling, and social control, sparking worries about misuse and discrimination in AI surveillance systems. These systems can inadvertently perpetuate biases found in the data they are trained on, resulting in discrimination against

¹ Filippo Raso and Oth., *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center Research Publication 01, 07, (2018),

https://dash.harvard.edu/bitstream/handle/1/38021439/201809_AIHumanRights.pdf?sequence=1&isAllowed=y.

² Markus Anderljung and Julian Hazell, *Protecting Society from AI Misuse: When are Restrictions on Capabilities Warranted?*, CORNELL UNIVERSITY, (2023). <https://doi.org/10.48550/arXiv.2303.09377>.

certain groups such as minorities or dissenters. Specifically, facial recognition technology has come under scrutiny for its possible role in profiling based on race and enabling widespread surveillance.³

Moreover, The rise in AI-powered surveillance technology has sparked fears of increasing government control and diminishing civil liberties. Continuous monitoring and tracking could lead to the loss of privacy, stifling opposition and restricting freedom of speech and assembly. To mitigate these risks, stringent regulations and safeguards are needed to ensure the ethical use of AI surveillance systems. This includes establishing rules for data collection, storage, and usage, as well as implementing measures to prevent discrimination and misuse. Increasing public awareness about the implications of AI surveillance and prioritizing transparency and accountability in its development and implementation are essential steps to safeguarding individual rights and freedoms.⁴

Legal Framework for AI and Human Rights:

Globally, human rights laws extend to AI, influencing fundamental rights. The United Nations' Business and Human Rights Principles hold companies accountable for AI practices impacting human rights. Nationally, countries grapple with crafting regulations addressing AI's impact on privacy and rights. GDPR shapes data protection laws, emphasizing consent and security. Despite efforts, global AI regulations face challenges due to rapid technological advancements, requiring adaptable frameworks to preserve human rights.⁵

The legal framework for AI involves regulating systems to ensure safety, security, and reliability. This includes setting standards for design, development, testing, and deployment, along with monitoring mechanisms. Addressing risks like bias and privacy violations is crucial, necessitating legal safeguards. Transparency and accountability promotion are vital, requiring organizations to disclose AI system details. Redress mechanisms are needed for AI-caused harm or rights violations. Liability and responsibility for AI systems must be clarified within the legal framework. Determining legal responsibility for developers, manufacturers, owners, and users is essential for accountability and legal recourse in cases of harm or rights violations.⁶

³ David Leslie and Oth., *Artificial intelligence, human rights, democracy, and the rule of law: a primer*, SSRN ELECTRONIC JOURNAL, (2021), <https://doi.org/10.2139/ssrn.3817999>.

⁴ *Id.*

⁵ Rajan Rayhan and Shahana Rayhan, *AI and Human Rights: Balancing Innovation and Privacy in the Digital Age*, RESEARCHGATE 1, 11-12, (2023),

https://www.researchgate.net/profile/RajaRayhan/publication/372743882_AI_and_Human_Rights_Balancing_Innovation_and_Privacy_in_the_Digital_Age/links/64c525b6cda2775c03d23cd4/AI-and-Human-Rights-Balancing-Innovation-and-Privacy-in-the-Digital-Age.pdf.

⁶ Rowena Rodrigues, *Legal and human rights issues of AI: Gaps, challenges and vulnerabilities*, 4 JOURNAL OF RESPONSIBLE TECHNOLOGY 1, 1-12, (2020), <https://doi.org/10.1016/j.jrt.2020.100005>.

Technological Solutions for Enhancing Privacy Against AI:

As AI surveillance technologies like facial recognition and gait analysis become increasingly prevalent, there is a growing worry about the infringement on privacy and freedom. To address these concerns, experts are developing new ways to safeguard personal data and mitigate the potential harms of surveillance technology. Their goal is to empower individuals with the means to shield their information and mitigate the negative effects of AI monitoring. One promising approach is the development of privacy-enhancing technologies (PETs). These technologies use cryptographic techniques, secure communication protocols, and anonymization methods to make sure that data is collected, stored, and processed in a way that preserves privacy. For example, homomorphic encryption allows data to be processed while still encrypted so that sensitive information cannot be accessed by unauthorized individuals.⁷

Another focus area is the development of AI systems that prioritize privacy. This involves designing algorithms that can analyze data without revealing individual identities. Techniques like differential privacy and federated learning enable data analysis to be done in a distributed manner, reducing the likelihood of personal information being exposed. The popularity of "privacy by design" is on the rise. This means integrating privacy considerations into the design and development of AI systems from the beginning. By including privacy-friendly features and safeguards early on, the risk of privacy breaches and misuse can be greatly reduced.⁸

Conclusion:

Navigating the intersection of artificial intelligence and human rights requires a careful balance between technological progress and individual freedoms. AI has the potential to advance human rights by improving access to education and healthcare, promoting social justice, and equality. However, ethical considerations, privacy risks, and job displacement must be taken into account. Developing transparent and explainable AI systems is crucial to preserving human dignity and autonomy. Regulatory bodies must enforce data protection laws and ethical guidelines for AI use in the criminal justice system, ensuring technology respects and upholds human rights. Collaborative discussions are essential to realize the benefits of AI without compromising fundamental rights.

⁷ Barnabás Székely, *Mitigating the Privacy Risks of AI through Privacy-Enhancing Technologies*, 11(2) SCIENTIA KIADÓ 1, 35-40, (2022), <http://real-j.mtak.hu/24664/7/ACTA-LegalStudies-112-2022.pdf#page=35>.

⁸ *Id.*