INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 3 | Issue 5 Art. 6

2024

Surveillance, Bias and Human Rights: The Case of Facial Recognition and Violation of Human Rights

G Darshita

Recommended Citation
G Darshita, *Surveillance, Bias and Human Rights: The Case of Facial Recognition and Violation of Human Rights*, 3 IJHRLR 151-164 (2024).
Available at www.humanrightlawreview.in/archives/.

Surveillance, Bias and Human Rights: The Case of Facial Recognition and Violation of Human Rights

G Darshita

Law Student, 4th Year, BBA.LL.B. (Hons.), School of Law, Christ (Deemed To Be University), Bangalore, India

Manuscript Received	Manuscript Accepted	Manuscript Published
09 Sept. 2024	14 Sept. 2024	17 Sept. 2024

ABSTRACT

The widespread adoption of Artificial Intelligence (AI) powered facial recognition technology has brought both benefits and significant risks. While this technology offers potential advantages in fields like security and law enforcement, it also presents a serious threat to human rights and equality. The inherent biases that exist within AI algorithms can lead to discriminatory outcomes in various areas of life, including the criminal justice system, healthcare, and social services. This paper analyses existing violations of human rights arising from the misuse of facial recognition technology and the inherent bias in artificial intelligence. The paper will delve into the inherent biases present in AI algorithms and its functions. These biases can lead to discriminatory outcomes, such as wrongful arrests, surveillance of marginalized communities, and restrictions on freedom of expression. The research will also examine the potential for Facial Recognition Technology (FRT) to be used for mass surveillance and the creation of digital authoritarian regimes. By drawing on interdisciplinary perspectives from law, ethics, and AI development, it advocates for policies that ensure accountability, transparency, and the protection of human rights in the use of FRT. This paper examines the ethical implications, inherent biases, and real-world applications of FRT, this research paper aims to contribute to a broader understanding of the potential risks and benefits of AI-driven surveillance. Therefore, it is crucial to address the issue of bias in AI-powered facial recognition technology. By developing more equitable and inclusive AI algorithms, implementing robust ethical frameworks, and ensuring transparency and accountability in the use of facial recognition

technology, we can mitigate the risks and maximize the benefits of this powerful tool.

KEYWORDS

Artificial Intelligence, Facial Recognition Technology, Human Rights Violations, Bias, Discrimination

1. INTRODUCTION

The advent of facial recognition technology has ushered in a new era of surveillance, promising enhanced security and efficiency. However, the widespread deployment of this technology raises profound concerns about privacy, civil liberties, and the potential for discrimination. Facial recognition poses a significant challenge to privacy and civil liberties due to its ability to remotely identify, track, and monitor individuals at scale. This unprecedented surveillance capability, combined with the increasing digitization and development of AI, empowers states to gain extensive insights into individuals' lives. This surveillance can be used to make decisions that affect various aspects of individuals' lives, including social welfare, healthcare, immigration, and law enforcement. The ability of states to monitor individuals and translate this information into decision-making processes directly impacting their lives represents a fundamental shift in state power and influence[1].

In addition to the concerns about privacy and civil liberties, facial recognition technology also raises concerns about bias and discrimination. Studies have shown that facial recognition algorithms can be biased against certain groups of people, such as people of colour and women. This bias can lead to discriminatory outcomes, such as wrongful arrests or denials of

[1] Chris Buckley and Paul Mozur, 'How China Uses High-Tech Surveillance to Subdue Minorities', The New York Times.
(New York 22 May 2019).

services. The widespread adoption of facial recognition technology has significant implications for human rights and democratic societies. While there is a need to balance the benefits of this technology with the risks, it is clear that more robust safeguards and ethical considerations are necessary to ensure that facial recognition is used responsibly and in a way that respects human rights[2]. This paper delves into the intersection of surveillance, bias, and human rights, focusing specifically on the case of facial recognition. It examines the ways in which facial recognition technology can infringe upon fundamental human rights, such as the right to privacy, freedom of expression, and equality before the law. Moreover, the paper explores the inherent biases embedded in facial recognition algorithms, which can disproportionately impact marginalized communities.

2. ORIGIN AND GROWTH OF HUMAN RIGHTS

The Universal Declaration of Human Rights (UDHR) recognizes the inherent dignity and equal rights of all individuals as the foundation for peace and justice[3]. However, the precise nature and role of human rights in international law remain debated, with differing interpretations of what constitutes a "right" and how they should be enforced[4]. The concept of human rights is deeply intertwined with ethics and morality. Rights that reflect societal values are more likely to be successfully implemented. Positive rights are those enshrined in legal systems, while moral rights may not be legally enforceable. While positive rights can be easily

[2] Daragh Murray, 'Facial recognition and the end of human rights as we know them?', Netherlands Quarterly of Human Rights 2024, Vol. 42(2) 145–152
[3] UN General Assembly, Resolution 217A (III), Universal Declaration of Human Rights, A/RES/217(III) (December 10, 1948).
[4] Shestack, Jerome J., 'The Jurisprudence of Human Rights', in Theodor Meron (ed.), Human Rights in International Law: Legal and Policy Issues (Oxford, 1986; online edn, Oxford Academic, 22 Mar. 2012), https://doi.org/10.1093/acprof:oso/9780198255406.003.0003.

identified, inferring moral rights is subjective and depends on individual perceptions[5].

The origins of human rights can be traced to various sources, including religion, the nature of humanity, and societal structures. The Natural Law view posits that certain rights exist as a result of a higher law, transcending positive law. This perspective, associated with John Locke, influenced the establishment of universal human rights principles in the international community. Positivism, on the other hand, emphasizes state authority and limits the scope of rights to those recognized within legal systems[6]. Marxism, while acknowledging historical laws governing society, denies the existence of rights outside the legal framework.

Modern rights theories encompass a wide range of approaches, highlighting the need for a flexible legal system that can adapt to evolving circumstances. Policy-oriented movements focus on identifying and addressing factors that contribute to the creation and implementation of human rights. These movements emphasize human dignity as a central concept and advocate for a democratic distribution of values in the global community. The concept of human rights is complex and multifaceted, involving ethical, moral, and legal dimensions[7]. While the UDHR provides a foundational framework, ongoing debates and discussions are essential for understanding and advancing the protection of human rights in the international context.

The 19th century saw a limited recognition of human rights,

[5] Maurice Cranston, What are Human Rights? in Human Rights Reader (Walter Laqueur & Barry Rubin eds., 20th ed. 1989).
[6] D. Lloyd, Introduction to Jurisprudence, 4th edn, London, 1979, chapter 4.
[7] Shaw, M. N. (2003). International Law. Cambridge University Press. http://books.google.ie/books?id=cc3XzkFtIUC&printsec=frontcover&dq=Malcom+N+Shaw&hl=&cd=3&source=gbs_api.

primarily focused on specific issues like slavery, the treatment of prisoners of war, and the protection of aliens. While the League of Nations introduced some advancements, such as mandates for colonial territories and protections for minorities, it was still a far cry from a comprehensive international human rights framework. The horrors of World War II catalysed a significant shift in international thinking. The need for a system to prevent such atrocities and protect human rights became evident. This led to the creation of the United Nations and its human rights machinery, including the Universal Declaration of Human Rights, which articulated fundamental rights and freedoms for all individuals.

However, the challenges of enforcing human rights standards persisted. The rise of non-governmental organizations played a crucial role in advocating for human rights and holding governments accountable[8]. While international institutions and mechanisms have made progress, issues such as impunity and the use of domestic amnesty laws continue to hinder the effective protection of human rights.

3. GROWTH OF FRT

The market for FRT has experienced exponential growth, driven by its diverse applications. Businesses utilize it for authentication, payment authorization, employee monitoring, and targeted advertising. Governments and law enforcement agencies employ FRT to aid criminal investigations, conduct surveillance, and enhance security. However, this technological advancement comes at a cost. Facial recognition technology, though dating back

[8] C. Chinkin, 'The Role of Non-Governmental Organisations in Standard Setting, Monitoring and Implementation of Human Rights' in The Changing World of International Law in the 21st Century (eds. J. 1. Norton, M. Andendas and M. Footer), The Hague, 1998.

to the 1960s, gained significant traction in the early 1990s with government initiatives. However, its widespread adoption as a consumer product began around 2010 with the rise of social media platforms like Facebook. Despite its high accuracy rates, facial recognition technology suffers from bias due to unbalanced datasets. Many training databases predominantly feature white males, leading to algorithms that struggle to accurately identify individuals with darker skin tones, especially women. This bias stems from the technology's inability to effectively extract features from faces that differ from its primary training data[9].

Other factors contributing to bias include the design of devices that may not be sensitive to darker skin tones and the lack of consideration for diverse populations in the development of facial recognition algorithms. These limitations highlight the need for ongoing research and development to ensure the fairness and effectiveness of facial recognition technology. Facial recognition technology can identify individuals in digital images, both in real-time and retrospectively. While it may seem like a simple tool, its ability to track and monitor individuals poses significant privacy concerns. This technology enables states to identify individuals' locations, movements, and interactions, undermining individual anonymity and altering the power balance between states and citizens. Facial recognition uses machine learning to create biometric templates of faces and compare them to reference databases. Both live and retrospective facial recognition raise privacy concerns, as they allow states to track individuals' activities and generate detailed profiles.

One of the most pressing concerns is the lack of consent often

[9] Kaiser, L. (2024, February 21). UB computer science professor weighs in on bias in facial recognition software. University at Buffalo. https://www.buffalo.edu/news/tipsheets/2024/ub-ai-expert-facial-recognition-expert-ifeoma-nwogu.html.

associated with FRT. Individuals may find themselves unwittingly subjected to facial recognition, such as through public surveillance systems or aggregated databases. This raises questions about the extent to which personal information can be collected and used without explicit permission. The unique nature of facial data further exacerbates privacy risks. Unlike other forms of data, faces cannot be encrypted, making them vulnerable to breaches and potential misuse. A compromised facial recognition database could lead to identity theft, stalking, or harassment.

Transparency is another crucial issue[10]. The use of FRT without individuals' knowledge or consent undermines their privacy rights. Moreover, the ability to capture facial scans remotely and secretly poses additional concerns. Technical vulnerabilities also exist. FRT systems can be susceptible to spoofing, where individuals attempt to masquerade as others using images or 3D masks. Additionally, inaccuracies in facial recognition algorithms can lead to false positives, potentially resulting in wrongful arrests or other negative consequences.

To address these concerns, various regulations and guidelines have been introduced worldwide. While some jurisdictions have focused on regulating government entities, others have sought to establish broader frameworks for the private sector. However, the rapidly evolving nature of FRT and its widespread adoption present challenges in ensuring effective oversight. To mitigate privacy risks and promote responsible FRT usage, organizations should adhere to specific principles. These include obtaining explicit consent, using facial recognition data ethically, ensuring transparency, implementing robust data security measures,

[10] Ante Novokmet, Zvonimir Tomicic & Ivan Vidakovic, Facial Recognition Technology in EU Criminal Justice - Human Rights Implications and Challenges, 7 ECLIC 525 (2023).

prioritizing privacy by design, maintaining data integrity, and fostering accountability.

4. BIAS OF FRT

"Machine learning is a method of data analysis that automates analytical model building."[11] Facial recognition technology, despite its potential applications, has been shown to be biased against certain demographic groups. Machine Learning is a subset of artificial intelligence that enables computers to learn from data and improve their performance on a specific task without being explicitly programmed. This involves training algorithms on large datasets, allowing them to identify patterns and make predictions or decisions[12]. This process of developing patterns and categories is the crux of machine learning.[13]

Studies have revealed that the error rates for this technology vary significantly based on race and gender[14]. For example, darker-skinned women are more likely to be misidentified compared to light-skinned men. This bias has serious implications for law enforcement and the criminal justice system, which already disproportionately target and incarcerate people of colour. Furthermore, the prevalence of facial recognition technology in law enforcement has exacerbated existing racial disparities[15]. People of colour are more likely to be arrested for minor crimes, leading to a higher representation of their faces in mugshot databases. This increases the likelihood of misidentification and

[11] Machine Learning: What It Is and Why It Matters, SAS, https://www.sas.com/en_us/insights/analytics/machine-learning.html.
[12] Mitchell, Tom M., *Machine Learning* (1997)
[13] Yufeng Guo, The 7 Steps of Machine Learning, MEDIUM: TOWARDS DATA SCI. (Aug. 31, 2017), https://towardsdatascience.com/the-7-steps-of-machine-learning2877d7e5548e.
[14] Buolamwini, Joy & Gebru, Timnit. "Gender Shades: Algorithms in Our Everyday Lives." MIT Media Lab (2018).
[15] ACLU-MN. "Kylese Perryman Case." https://www.aclu-mn.org/en/news/aclu-mn-suing-after-wrongful-arrest-innocent-man.

wrongful arrests. Additionally, police surveillance cameras are disproportionately installed in Black and Brown neighbourhoods, further perpetuating systemic racism.

A study conducted by the National Institute of Standards and Technology (NIST) evaluated 189 FRT algorithms and found that the majority exhibited higher false positive rates for non-white and traditionally-female faces, particularly in one-to-many matching scenarios[16]. This underscores the potential consequences of using biased FRT systems in applications such as law enforcement, where false accusations can have serious implications. While some FRT programs may exhibit minimal bias, the overall issue remains a concern. Organizations deploying FRT should carefully research and scrutinize the specific algorithms they use to ensure they are aware of potential limitations and biases[17]. It is crucial to recognize that technology is not inherently neutral. It is created by people who carry biases, and these biases can be reflected in the technology itself[18].

Addressing algorithmic bias in FRT requires a multifaceted approach[19]. Program designers must strive to create more diverse and representative training datasets. Additionally, ongoing evaluation and monitoring of FRT systems are crucial to identify and mitigate biases as they emerge. By acknowledging and

[16] See Steve Lohr, Facial Recognition Is Accurate, If You're a White Guy, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facialrecognition-race-artificial-intelligence.html.
[17] Peter N. K. Schuetz, Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework, 39 MINN. J.L. & INEQ. 221 (2021).
[18] ACLU. "Overpolicing and Racial Bias:
How Police Surveillance Reinforces Inequality."
https://www.aclu.org/issues/racial-justice/race-and-criminal-justice/racial-profiling.
[19] Clare Garvie & Jonathan Frankle, Facial-Recognition Software Might Have a Racial Bias Problem, ATLANTIC (Apr. 7, 2016), https://www.the atlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognitionsystems/476991/.

addressing these challenges, we can harness the power of FRT while minimizing its potential for harm.

5. EFFECTS OF FACIAL RECOGNITION ON HUMAN RIGHTS

Facial recognition technology, while offering advancements in security and efficiency, also raises significant concerns about human rights. Beyond the direct impacts on privacy and discrimination, the pervasive surveillance enabled by this technology can have far-reaching consequences for individuals and society as a whole. One of the most concerning effects is the phenomenon of chilling effects[20]. When individuals believe they are constantly being watched and monitored, they may modify their behaviour to avoid potential repercussions. This can lead to self-censorship, limiting freedom of expression and association. Individuals may avoid attending certain events, joining specific organizations, or participating in political activities for fear of being identified and targeted. These chilling effects can have profound implications for personal development and democratic participation[21]. The ability to explore new ideas, challenge assumptions, and engage with diverse perspectives is crucial for forming a well-rounded identity. When individuals feel constrained by surveillance, their ability to experiment and grow is hindered.

Moreover, the rights to privacy, freedom of expression, and assembly are interconnected and essential for fostering a vibrant and democratic society. Surveillance can undermine all of these rights simultaneously. For instance, the anonymity that allows individuals to engage with different ideas freely can be

[20] Supra 2.
[21] Amy Stevens and others, 'I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe' (2023) 1 Big Data & Society 1, 2.

compromised by facial recognition technology. This can discourage individuals from seeking out new information or participating in public gatherings. The human rights implications of facial recognition extend far beyond privacy and discrimination. The chilling effects and broader societal impacts must be carefully considered as we navigate the complex landscape of technological advancement and individual freedoms.

While the concept of interconnected and interdependent rights is frequently acknowledged in human rights law, the reality is that cases are typically examined on a right-by-right basis. This approach, known as judicial minimization, can lead to an incomplete analysis of the broader impacts of human rights violations. In cases of Glukhin v. Russia[22], courts have often focused solely on the right to privacy, neglecting to consider the chilling effects on other rights such as expression and assembly. Similarly, in cases involving facial recognition technology, the European Court of Human Rights has acknowledged the potential for chilling effects but has not conducted a thorough analysis of their impact.

To address these limitations, a new approach is needed that considers the cumulative harm caused by violations of multiple rights. This approach, known as compound human rights harm, focuses on the overall impact of a measure on a range of rights rather than examining each right in isolation[23]. By adopting a compound human rights harm lens, courts can better grapple with the complex issues raised by digital technologies. This approach can help to ensure that human rights law remains relevant in the digital age and provides adequate protection for

[22] Glukhin v. Russia 11519/20.
[23] Supra 2.

individuals in the face of new challenges.

6. CONCLUSION

Human rights law faces significant challenges in adapting to the realities of facial recognition and other digital technologies. One major challenge lies in the traditional focus on after-the-fact remedies[24]. To effectively address human rights concerns in the digital age, a proactive approach is needed that involves engaging with decision-making processes and building in human rights compliance from the outset. This requires a shift in mindset for human rights lawyers, who must become more involved in political processes.

Another challenge is the complexity of compound human rights harm. While the concept of interconnected rights is essential, developing human rights law to address broader societal impacts requires a deeper understanding of societal structures and processes. This necessitates interdisciplinary collaboration between human rights lawyers and experts from the humanities and social sciences.

Furthermore, the types of harm caused by digital technologies, such as chilling effects, differ from traditional human rights violations. These harms are often more difficult to identify and document, as they may not be immediately apparent and can manifest over time. This requires a rethinking of how human rights harm is understood and addressed in legal frameworks. To meet these challenges, human rights law must evolve. By adopting a more proactive approach, engaging in interdisciplinary collaboration, and adapting to the complexities of digital harm,

[24] Daragh Murray, 'Police use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Framework Law' (2024) Modern Law Review.

human rights law can play a crucial role in shaping a just and equitable digital society.