Human Rights in the Age of Surveillance: Legal Implications of Biometric and Facial Recognition Technologies

[1]Dr. Sundarapandiyan Natarajan, [2]Dr. Kumar Prasant Shekhar, [3]Prof. (Dr.) Rajesh Kumar, [4]S.Suresh Kumar, [5]Prof. (Dr.) Ashwani Kumar Dwivedi, [6]Dr. Ashutosh O. Lanjewar

[1]Professor and Head, DoMS, Adithya Institute of Technology, Coimbatore, T.N., India, Email: nt_sundar@yahoo.com, ORCID-ID: 0000-0002-1303-2947
[2]Assistant Professor, Department of History, Satyawati College(Evening), University of Delhi, Email: Prasant.history@satyawatie.du.ac.in
[3]Dean, University School of Law, Guru Kashi University, Bathinda, Punjab, Email: dr.rajeshkumar0601@gmail.com, ORCID-ID: 0000-0002-5254-3552
[4]Ph.D. Research Scholar, Faculty of Law, Kakatiya University, Warangal,Telangana, India, Email: sskv73@gmail.com
[5]Professor and Associate Dean, Faculty of Law, SGT University, Gurugram, Haryana, India, Email: ashwani.dwivedi89@gmail.com
[6]Associate Professor , Department of Artificial intelligence, J. D. College of Engineering and Management, Nagpur, Maharashtra, India, Email: ashutoshlanjewar39@gmail.com

ABSTRACT

The development of biometric technology and facial recognition technology is happening more rapidly than the legislation attempting to regulate the same, thus leaving much at stake regarding the balance between security concerns and human rights. This paper addresses legal aspects of biometrics in terms of privacy, equality, and the right to freedom of expression and assembly. Secondary data has been used in order to carry out this analysis through surveillance camera index, surveys, and reports of regulatory enforcement. There are three major themes that can be identified: universal adoption of biometrics-enabled surveillance architecture; increasing divergence between context-specific trust and demographic accuracy; and regulatory fragmentation with respect to reactive and preventive enforcement measures. It is argued that the level of legal certainty, algorithmic accountability, and remedial measures in place is still underdeveloped in relation to the deployment. It is proposed in the paper that a rights-based and coherent approach to regulation is needed.

Keywords: facial recognition technology, biometric surveillance, human rights, data protection, AI Act, algorithmic bias

1. INTRODUCTION

Biometrics and facial recognition technologies have transitioned from the domain of science fiction to being used for routine governance within a period of only about two decades. The airports, transit networks, retail businesses, educational institutions, and policing agencies around the world make use of automated systems that digitize a person's face (Qandeel, 2024). Such developments have produced positive benefits in the form of efficient border control and crime prevention, but they have also led to the emergence of a considerable amount of case law and literature on the issue of serious human rights violations (Wang et al., 2024). Some of the main rights that have been violated include those of privacy and data protection, non-discrimination, and freedom of speech and assembly (Gabrielli, 2025).

The legal response to the problem has not been consistent. For example, the European Union has passed the Artificial Intelligence Act, which is the first attempt to categorize biometric identification as either a high-risk or

prohibited activity (Jung and Virgil, 2024). In other regions, the legal measures include a combination of state-level statutes like the Biometric Information Privacy Act in Illinois, whereas others have increased biometric surveillance with limited legal restrictions (Lynch, 2024). The aforementioned inconsistencies present an issue that the paper aims to address, namely, how well current legislation protects human rights from the potential threat associated with the use of biometric technologies and facial recognition systems.

The paper is structured into six sections. In section two, the literature review on biometrics and human rights is presented. Section three gives the methodology of the study, while section four presents a thematic analysis of data with figures and tables. Section five analyses the implications for law and policy, while section six presents' recommendations for improved regulatory structure.

2. LITERATURE REVIEW

2.1 Privacy, Surveillance, and the Rule of Law

There is a substantial body of law literature that views facial recognition technology (FRT) from the perspective of states' obligations in terms of respecting, protecting, and fulfilling human rights. According to Qandeel (2024), FRT technology represents an "unacceptable risk" technology under evolving EU doctrine due to interference with individuals' privacy, equality, and dignity rights in the use of biometric identification. The same is reflected in Gabrielli (2025), who conducts an analysis of the European Court of Human Rights case decision of Glukhin v Russia, which marks the first time the ECtHR made its decision related to FRT. She demonstrates that the interference with the right to privacy and freedom of expression of a peaceful protester through FRT was not necessary and proportionate, and the mass-surveillance jurisprudence developed for bulk communications interception has been applied to biometric identification in the physical public sphere.

Wang et al. (2024) note the same about the inadequacy of laws currently in force in terms of meeting rigorous academic criteria and international human rights standards, emphasizing that it is necessary to move from data protection compliance alone to an ethics-and-rights-based approach in governance. Fussey (2025) identifies the ultimate impact of FRT that it changes the essence of suspicion itself because, through turning similarities into leads for investigation, it changes discretion and presumption of innocence.

2.2 Algorithmic Bias and Discrimination

The second theme addresses the issue of demographic accuracy discrepancies in FRT. The paper by Yucer et al. (2024) is the most thorough taxonomical analysis of racial bias in face recognition, where the authors conclude that performance differences among races continue to persist throughout the process chain, and most of the bias reduction methods involve race classification, which may be scientifically controversial. Similar findings are presented by de Oliveira et al. (2025), where the authors give fourteen recommendations on access control systems. Criticism of this nature is furthered by Judijanto (2025), who adopts a decolonial approach to show how racial bias is a result of the epistemic supremacy of Western-designed algorithms that are incapable of recognizing non-Western faces properly. An economic critique, according to Kasy (2024), demonstrates how the fairness measures are in favour of the decision-maker and not the welfare of the disadvantaged group.

2.3 Regulatory and Enforcement Responses

Comparative literature on regulation exhibits considerable differences. According to Lynch (2024), although there is legislation on the issue, it appears that the concept of principled regulation is not thoroughly mapped out in comparison with scholarship, especially concerning retention limits and children's biometric information. Jung and Virgil (2024) use the confidentiality-integrity-availability-authorisation-accountability framework in the analysis of biometric laws in the GDPR, Illinois BIPA, Brazilian LGPD, and South African POPIA, and find great differences in the severity of law enforcement.

2.4 Chilling Effects and Collective Rights

Murray et al. (2024) offer scarce qualitative insights into how surveillance operates as a source of chilling effect for civic activities based on interviews with 44 individuals in Uganda and Zimbabwe. These studies show the connection between surveillance and self-censorship through the analysis of empirical data rather than assumptions that had been raised before in scholarly works. Haley (2025) and Haley and Burrell (2025) suggest

that biometrics like real-time crime centers can be helpful in public safety efforts, but there is a possibility of over-policing of vulnerable groups of people without any independent controls. All these publications confirm that there is more to human rights consequences of biometric surveillance than just data protection issues.

3. METHODOLOGY

The current study uses qualitative desk-based research, which is based solely on secondary data and where no primary data was collected. There were three types of secondary sources used. First, peer-reviewed literature on the legal and social issues associated with biometric technology from 2024 onwards was found via Frontiers, MDPI, Oxford Academic, Cambridge Core, ACM Digital Library, and other relevant databases, with emphasis on open-access articles concerning the legal and human rights implications of biometric technology; fifteen articles in total formed the basis of analysis. Second, secondary quantitative data on surveillance infrastructure and public perceptions were taken from Comparitech's global CCTV density survey reports and Pew Research Center surveys. Third, data on legislation and enforcement were taken from professional law-related sources covering GDPR enforcement and comparative biometric laws.

Instead of analysing the sources serially, the data were analysed thematically, using the well-established method of identifying patterns among disparate secondary sources and categorizing them into overarching analytical themes. The three themes were identified through an inductive process involving patterns found within the literature and datasets: the size of biometric-enabled infrastructure, the discrepancy between public trust and algorithmic accuracy, and the reactive nature of regulatory enforcement. This secondary-source analysis is appropriate for a paper aimed at synthesizing research rather than conducting primary analysis. The limitations are related to the reliance on original reporting decisions, the focus of survey data on the US and Europe, and the delay between legal scholarship and implementation practice, which was addressed by focusing on 2024-2026 datasets.

4. DATA ANALYSIS

Secondary data was analysed using thematic analysis. Themes inductively emerged from the data sets related to the surveillance infrastructure, public opinion, accuracy of algorithms, and enforcement: (i) the global scale and reach of biometric-capable infrastructure; (ii) the gap between public trust and algorithmic accuracy; and (iii) regulatory fragmentation and reactive enforcement. Each theme is presented below with its supporting figures and tables.

4.1 Theme One: The Global Scale and Reach of Biometric-Capable Infrastructure

The latest global study on the distribution of surveillance cameras conducted by Comparitech (2025) demonstrates that the density of CCTV usage varies significantly from one country to another and is not limited only to authoritarian regimes (Figure 1). India's urban centers like Hyderabad (79 cameras per 1,000 people) and Indore (72 per 1,000) are amongst the most closely surveilled cities in the world, surpassing even the majority of US cities (Comparitech, 2025; Visual Capitalist, 2026). While Atlanta, the US capital with the highest number of cameras per capita, has about 50 cameras per 1,000 people, London has merely 13.4 per 1,000 people overall, with much higher density in particular boroughs like the City of London (75.3 per 1,000) (Comparitech, 2025). Importantly for reasons of legal relevance, this distribution means that biometric-enabled infrastructures are being deployed within democratic and non-democratic states (Qandeel, 2024). The issue as to whether these infrastructures can be lawfully associated with facial recognition analytics is hence a near-universal governance problem, rather than one restricted to a select few states. Indeed, as seen from Table 1, even those jurisdictions with advanced data protection traditions have failed to correspondingly increase their pre-authorisation requirements alongside the growth of infrastructures (Qandeel, 2024; Lynch, 2024; Jung and Virgil, 2024; Gasiokwu et al., 2025).

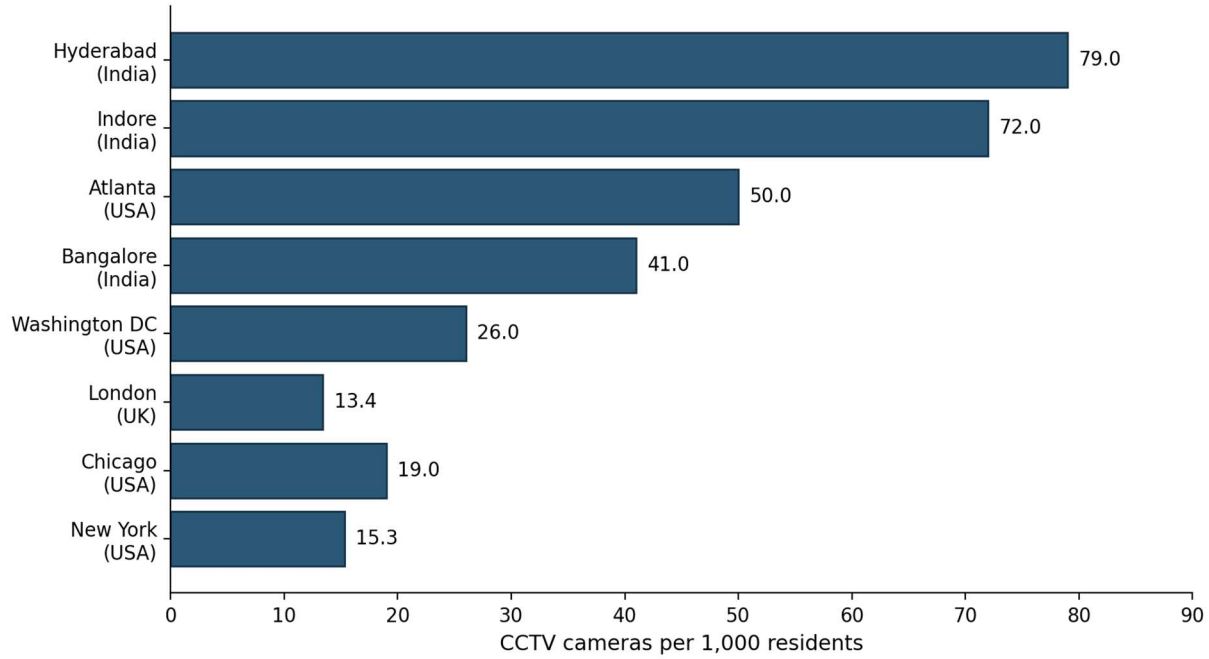

Figure 1: Public CCTV camera density in selected global cities (2024-2025)

Source: Comparitech (2025) global surveillance camera studies; Visual Capitalist (2026), compiled by author.

Table 1. Comparative Regulatory Frameworks for Biometric/Facial Recognition Technology

Jurisdiction	Primary Legal Instrument	Approach to Real-Time FRT	Independent Oversight Body	Key Gap Identified in Literature
European Union	AI Act (2024); GDPR	Prohibited in publicly accessible spaces, subject to narrow law-enforcement exceptions	AI Office; national market-surveillance authorities	Broad exceptions; GDPR enforcement remains largely reactive (Gasiokwu et al., 2025)
United States	State statutes (e.g., Illinois BIPA); no federal biometric law	Permitted; regulated in a minority of states only	State attorneys-general; private right of action (Illinois only)	Fragmented coverage; most states lack biometric-specific protection (Jung and Virgil, 2024)

Jurisdiction	Primary Legal Instrument	Approach to Real-Time FRT	Independent Oversight Body	Key Gap Identified in Literature
United Kingdom	Data Protection Act 2018; common law (Bridges v South Wales Police)	Permitted subject to case-by-case judicial review	Information Commissioner's Office	No FRT-specific statute; protection relies on litigation (Lynch, 2024)
China	Personal Information Protection Law	Extensively deployed; broad public-security consent exceptions	Cyberspace Administration of China	Public-security exceptions largely undefined (Qandeel, 2024)

Source: compiled by author from Qandeel (2024), Lynch (2024), Jung and Virgil (2024), and Gasiokwu et al. (2025).

4.2 Theme Two: The Trust-Accuracy Gap

Another issue relates to the disparity between the context-specific public trust and the algorithmic accuracy being demonstrated. The data from the Pew Research Centre reveals that the public trust in FRT is highly context-specific (Figure 2), where the majority of the American adults see the use of FRT for public safety by the police (53% support) and payment security by the retailers (53% support) as acceptable, but not for commercial surveillance purposes; only 40% support employers' attendance tracking and 25% advertisers' use (*Pew Research Center, 2022)*. This trend aligns with contextual integrity concerns mentioned in the literature as well; people care less about the practice of biometric identification as such and rather about its application in contexts different from those in which the information was shared (Wang et al., 2024). There is also an unequal distribution of trust: Blacks and Hispanics are significantly more likely than whites to expect wrongful arrests to become more common.

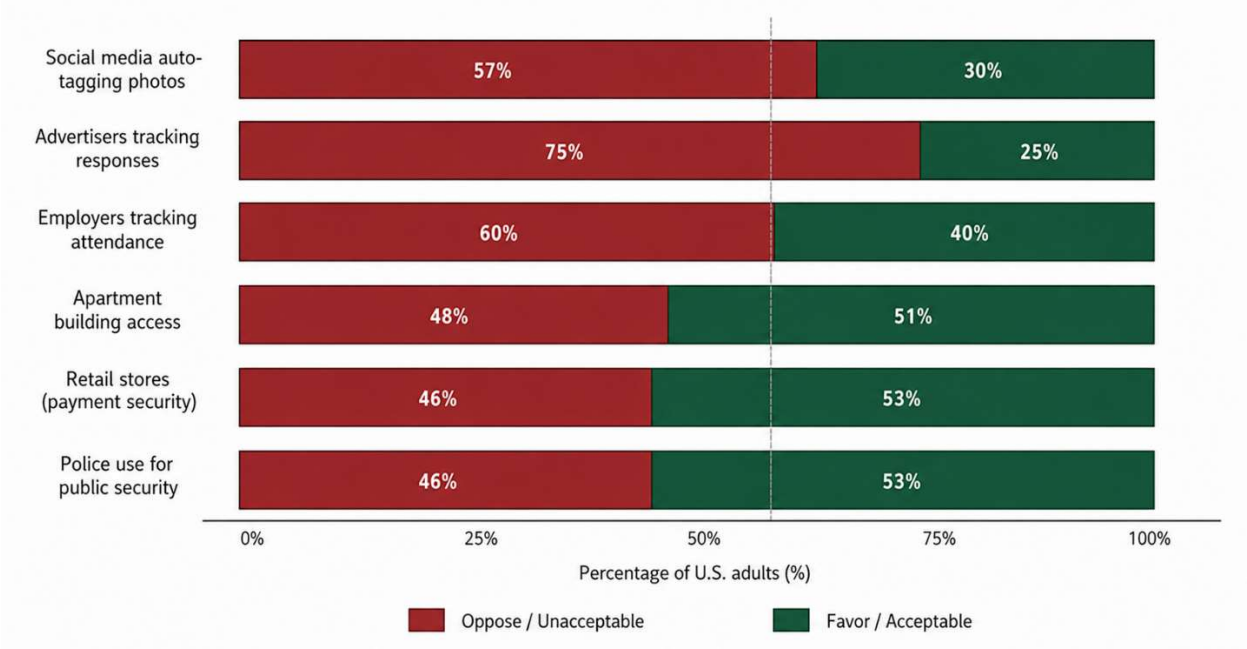

Figure 2: US public attitudes towards facial recognition

Source: Pew Research Center (2022, 2023) surveys on facial recognition technology, compiled by the author.

The issue is confirmed by figures on the disparity between accuracy rates. Based on Gender Shades accuracy-disparity figures used and repeated in the literature by Yucer et al. (2024) and de Oliveira et al. (2025), Figure 3 demonstrates that facial analysis systems were wrong about darker-skinned women in 34.7% of cases, while for darker-skinned men, in 12%, lighter-skinned women, in 7.1%, and lighter-skinned men, in 0.8%. It should be noted that the Gender Shades study is focused on gender classification rather than identity matching. However, according to Yucer et al. (2024), subsequent studies have shown similar rates of bias with regard to one-to-one and one-to-many identity matching, which are critical for law enforcement. As false-positive identification is the type of mistake that leads to unjustified detention, an increased false-positive rate for particular groups indicates additional burden on the right to liberty and protection from discrimination for those particular groups.

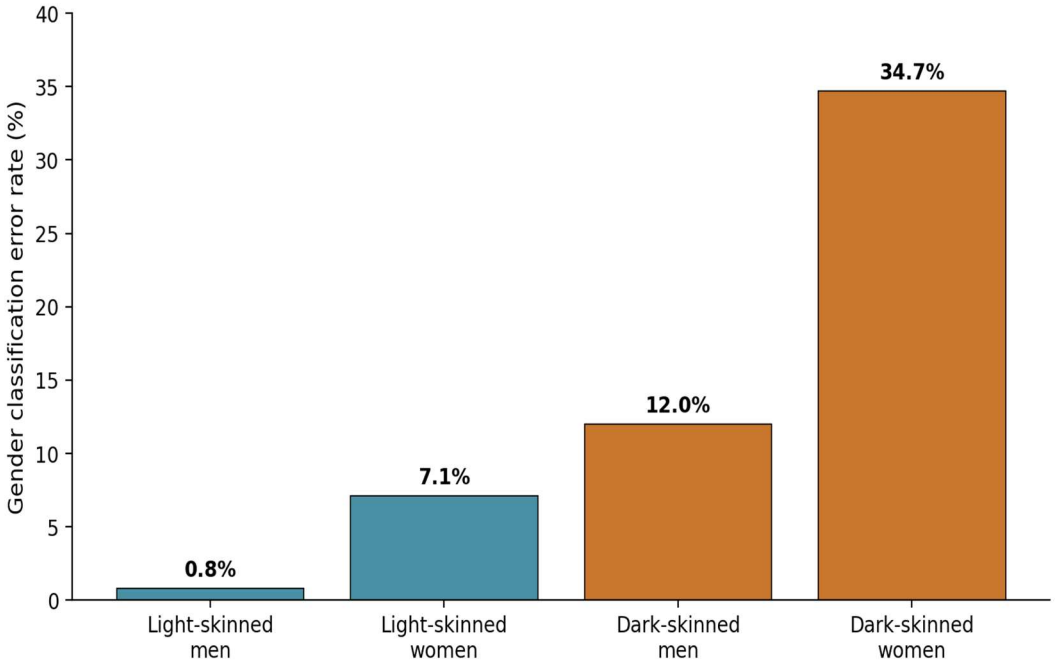

Figure 3: Demographic disparities in commercial facial analysis accuracy

Source: Buolamwini & Gebru (2018) benchmark, as reported and synthesised in Yucer et al. (2024) and de Oliveira et al. (2025), compiled by the author.

4.3 Theme Three: Regulatory Fragmentation and Reactive Enforcement

Theme three is that of legislative ambition versus enforcement practice. As Table 1 indicates, there is not currently any jurisdiction that has in place all three elements of comprehensive ex ante authorisation, the necessity-and-proportionality test, and an adequately resourced independent oversight mechanism. Of those listed, the EU AI Act is perhaps the most ambitious in banning real-time remote biometric identification in public spaces, subject to narrow law enforcement exceptions; however, Gasiokwu et al. (2025) point out that GDPR enforcement is reactive in nature. Reactive enforcement is illustrated in Table 2, where data protection authorities in France, Italy, and the Netherlands have imposed fines on Clearview AI for scraping billions of images without consent, amounting to between EUR 20 million and EUR 30.5 million in fines, while in Spain, a supermarket chain was fined EUR 2.52 million. These measures were only taken after large-scale collection and utilization had happened to demonstrate, in line with Gasiokwu et al. (2025) and Qandeel (2024), that present legal mechanisms mainly serve as deterrent measures ex post than preventive measures ex ante.

Table 2. Selected Data-Protection Enforcement Actions Involving Biometric/Facial Recognition Data (2022–2024)

Regulator (Country)	Company	Violation	Fine (approx.)
CNIL (France)	Clearview AI	Unlawful large-scale scraping of facial images without consent	EUR 20 million

Regulator (Country)	Company	Violation	Fine (approx.)
Garante (Italy)	Clearview AI	Unlawful biometric data processing; ordered data erasure	EUR 20 million
Autoriteit Persoonsgegevens (Netherlands)	Clearview AI	Unlawful retention of biometric data of Dutch citizens	EUR 30.5 million
AEPD (Spain)	Mercadona (supermarket chain)	Deployment of in-store FRT without a lawful basis or adequate transparency	EUR 2.52 million

Source: compiled by author from VinciWorks (2024), GDPR Local (2025), and Vista InfoSec (2026) regulatory trackers.

5. DISCUSSION

The three themes in section four validate the related issues of law highlighted in the literature review. Firstly, the worldwide spread of biometric-capable technologies means that the governance gap recognized by Qandeel (2024) as existing between fast technology deployment and slow development of regulations is, in fact, a universal issue rather than an exception of autocratic countries. Secondly, it proves the need for universal governance mechanisms as stated by Wang et al. (2024).

Second, there is a legal implication of the trust-accuracy discrepancy, which states that the communities that are least trusting in the deployment of police FRT systems, because of their justified expectations of higher rates of wrongful arrests, are the communities for which the empirical evidence demonstrates the highest rates of false positives. This connection between subjective risk perception and objective accuracy statistics makes discrimination arguments made in the literature (Yucer et al., 2024; Judijanto, 2025) even more credible and implies that proportionality considerations according to laws such as the ECHR or EU AI Act require accuracy auditing of demographics.

Thirdly, the theme of reactive enforcement means that even the GDPR, which is the most sophisticated form of data protection regime, operates as a deterrent acting ex post facto, and not as a licensing system that can prevent illegal implementation of the technology beforehand. In this regard, the observation made by Murray et al. (2024) is that surveillance chill effects accumulate and cannot be undone because, by the time the regulator applies the fine, the chilling effect on assembly and speech may have set in. The case of Glukhin v Russia, analysed by Gabrielli (2025), implies that the human rights courts may find themselves forced to look at the ability of the system to retain and analyse the biometrics as the key interference point.

The three themes combined point to recommendations in the literature (Kasy, 2024; Fussey, 2025) for the move away from a technology-specific checklist approach to one based on human rights that are defined as necessary, proportionate, and independent of oversight. This would include, at least: pre-deployment mandatory assessment of the impacts of the algorithms used and of bias or accuracy; enforceable rules regarding data retention and limitations on purposes, especially as regards the processing of biometric data of children (Lynch, 2024); and remedies to those wrongfully surveilled, including effective domestic remedies recognized under international human rights law (Qandeel, 2024). The findings also demonstrate that vendor self-regulation is inadequate, given that the worst violations occurred despite the vendor's own principles of ethics.

These caveats need to be mentioned. The secondary survey datasets are limited to the US, and the surveillance-density datasets favour the jurisdictions that publicly report their data and are therefore likely under-representing other jurisdictions. The accuracy-disparity ratios, which are very well-established, are based on a benchmark year of 2018; newer machine learning algorithms have been able to close some of these disparities in spite of the continued presence of disparate impact among these newer studies.

6. CONCLUSION

In this paper, we have looked into the legal consequences of the use of biometric and facial recognition technology on human rights using a thematic analysis of the secondary data on the surveillance infrastructure, public opinion, accuracy of algorithms, and legal enforcement. There were three themes that came up from the analysis. The first theme is that there has been a global growth in the surveillance infrastructure, but there has not been a corresponding growth in laws that could oversee its development. The second theme is that the demographic accuracy problems with FRT technology are in line with groups that lack trust and see themselves at a higher risk of being wrongfully arrested. The third theme is that even when the data protection laws are advanced, their enforcement comes only after the violation of privacy. The above-mentioned results suggest that existing legislation, whether a risk-based approach employed by the European Union, US state laws, or any other less restrictive systems in other places around the world, has not managed to achieve the right balance between clear positive outcomes of biometric authentication and potential negative consequences for privacy, equality, and freedom of speech and assembly. An effective way forward would involve mandating a human rights and bias-accuracy impact assessment prior to deployment, applying necessity and proportionality requirements based on emerging European Court of Human Rights case law, and creating independent monitoring entities to do this before deployment.

REFERENCES

Buolamwini, J., and Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

Comparitech. (2025). The world's most surveilled cities. https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

de Oliveira, A. M., Rodrigues, H. X., Nery, A. S., de Mendonça, F. L. L., and Junior, L. A. R. (2025). Influence of racial bias in the use of facial recognition applied to access control: A critical analysis. Research, Society and Development, 14(2), e3014248186. https://doi.org/10.33448/rsd-v14i2.48186

Fussey, P. (2025). Facial recognition. In M. Kaufmann & H. Mork Lomell (Eds.), De Gruyter Handbook of Digital Criminology (pp. 233–243). De Gruyter. https://doi.org/10.1515/9783111062037-028

Gabrielli, G. (2025). 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, 16(2), 514–541. https://doi.org/10.1017/err.2025.26

Gasiokwu, P. I., Oyibodoro, U. G., and Nwabuoku, M. O. I. (2025). GDPR safeguards for facial recognition technology: A critical analysis. International Research Journal of Multidisciplinary Scope, 6(1), 407–423. https://doi.org/10.47857/irjms.2025.v06i01.02025

GDPR Local. (2025). Biometric data GDPR compliance made simple. https://gdprlocal.com/biometric-data-gdpr-compliance-made-simple/

Haley, P. (2025). The impact of biometric surveillance on reducing violent crime: Strategies for apprehending criminals while protecting the innocent. Sensors, 25(10), 3160. https://doi.org/10.3390/s25103160

Haley, P., and Burrell, D. N. (2025). Integrating artificial intelligence into law enforcement: Socioeconomic and ethical challenges. SocioEconomic Challenges, 9(2), 60–77. https://doi.org/10.61093/sec.9(2).60-77.2025

Judijanto, L. (2025). Unmasking racial disparities: Epistemic injustice and bias in facial recognition systems. Scientia. Technology, Science and Society, 2(12), 1–15. https://doi.org/10.59324/stss.2025.2(12).01

Jung, Y., and Virgil, E. D. (2024). Analysis of legislative framework governing biometric data. Procedia Computer Science, 241, 48–55. https://doi.org/10.1016/j.procs.2024.08.009

Kasy, M. (2024). Algorithmic bias and racial inequality: A critical review. Oxford Review of Economic Policy, 40(3), 530–546. https://doi.org/10.1093/oxrep/grae031

Lynch, N. (2024). Facial recognition technology in policing and security: Case studies in regulation. Laws, 13(3), 35. https://doi.org/10.3390/laws13030035

Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., and Stevens, A. (2024). The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe. Journal of Human Rights Practice, 16(1), 397–412. https://doi.org/10.1093/jhuman/huad020

National Academies of Sciences, Engineering, and Medicine. (2024). Facial recognition technology: Current capabilities, future prospects, and governance. The National Academies Press. https://doi.org/10.17226/27397

Pew Research Center. (2022). Public views of police use of facial recognition technology. https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/

Pew Research Center. (2023). Americans' views on use of face recognition in the workplace. https://www.pewresearch.org/internet/2023/04/20/americans-views-on-use-of-face-recognition-in-the-workplace/

Qandeel, M. (2024). Facial recognition technology: Regulations, rights and the rule of law. Frontiers in Big Data, 7, 1354659. https://doi.org/10.3389/fdata.2024.1354659

VinciWorks. (2024). The biggest data protection, GDPR and AI stories of 2024. https://vinciworks.com/blog/the-biggest-data-protection-gdpr-and-ai-stories-of-2024/

Vista InfoSec. (2026). Privacy implications for GDPR & biometric data. https://vistainfosec.com/blog/gdpr-biometric-data-ethical-privacy/

Visual Capitalist. (2026). Ranked: The world's most surveilled cities. https://www.visualcapitalist.com/ranked-the-worlds-most-surveilled-cities-by-camera-density/

Wang, X., Wu, Y. C., Zhou, M., and Fu, H. (2024). Beyond surveillance: Privacy, ethics, and regulations in face recognition technology. Frontiers in Big Data, 7, 1337465. https://doi.org/10.3389/fdata.2024.1337465

Yucer, S., Tektas, F., Al Moubayed, N., and Breckon, T. P. (2024). Racial bias within face recognition: A survey. ACM Computing Surveys, 57(4), Article 105, 1–39. https://doi.org/10.1145/3705295