How to cite this article:
Besharatian, R., & Ghaffarpour, F. (2024). The Human Rights Impact of Biometric Surveillance: A Community-Based Study. *Journal of Historical Research, Law, and Policy, 2*(2), 17-24. https://doi.org/10.61838/jhrlp.2.2.3

Article history:
Original Research

Dates:
Submission Date: 11 February 2024
Revision Date: 15 March 2024
Acceptance Date: 28 March 2024
Publication Date: 01 April 2024

The Human Rights Impact of Biometric Surveillance: A Community-Based Study

1. Reza. Besharatian[1] : Department of Public Law, University of Kerman, Kerman, Iran
2. Fatemeh. Ghaffarpour[2*]: Department of Political Thought in Islam, University of Kerman, Kerman, Iran

*corresponding author's email: f7.ghaffarpour7@yahoo.com

ABSTRACT

This study aimed to explore the human rights impact of biometric surveillance through the lived experiences and perceptions of community members in Tehran. A qualitative research design was employed, utilizing semi-structured interviews with 27 participants recruited purposively from Tehran. Data collection continued until theoretical saturation was achieved. Interview transcripts were analyzed thematically using NVivo software to identify key themes related to privacy concerns, legal and ethical issues, social and community impacts, and technological factors. Four main themes emerged from the analysis. Privacy concerns dominated, with participants highlighting limited awareness of data collection, fears about data security breaches, surveillance-induced anxiety, behavioral modifications, and distrust of authorities. Legal and ethical issues revealed perceived regulatory gaps, challenges in obtaining genuine consent, and calls for accountable and ethical technology use. Socially, biometric surveillance was associated with discrimination, social exclusion, erosion of trust, low public awareness, and disproportionate effects on vulnerable groups. Technological factors, including accuracy limitations, data management practices, technological accessibility, system integration, user control deficits, and lack of transparency, further shaped participants' perceptions. These findings underscore the multifaceted human rights challenges posed by biometric surveillance in a context with evolving technological adoption but insufficient legal safeguards. The study demonstrates that biometric surveillance significantly impacts individuals' privacy, autonomy, and social well-being, particularly in settings lacking robust regulation and public engagement. Addressing these issues requires comprehensive legal frameworks, transparent and ethical technology deployment, enhanced public awareness, and inclusive governance models to safeguard human rights in the digital age.

Keywords: *Biometric surveillance, human rights, privacy, qualitative study, Tehran, data security, discrimination, technological ethics*

Introduction

The rapid advancement and proliferation of biometric surveillance technologies have introduced profound implications for individual privacy and human rights worldwide. Biometric surveillance encompasses the automated recognition of individuals based on their unique physiological or behavioral characteristics, such as fingerprints, facial features, iris patterns, and voice recognition (Jain, Ross, & Nandakumar, 2011). Governments and private sectors increasingly deploy such technologies for purposes ranging from national security and law enforcement to commercial applications and social control (Lyon, 2018). Despite their potential benefits in enhancing security and operational efficiency, biometric systems raise complex ethical, legal, and social concerns, particularly regarding the infringement of fundamental human rights.

Human rights frameworks, such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), enshrine the right to privacy, freedom from discrimination, and protection against arbitrary surveillance (United Nations, 1948; 1966). However, the deployment of biometric surveillance systems has sparked intense debates about the extent to which such technologies align with or violate these rights (Greenleaf, 2018). Critics argue that biometric surveillance can lead to pervasive monitoring, loss of anonymity, and unchecked data collection, thereby undermining the right to privacy and other civil liberties (De Hert & Papakonstantinou, 2018). Furthermore, concerns about bias and discrimination are prominent, as biometric systems have demonstrated inaccuracies disproportionately affecting racial minorities, women, and marginalized communities, which may exacerbate social inequalities and result in wrongful identification or targeting (Buolamwini & Gebru, 2018; Garvie, Bedoya, & Frankle, 2016).

Despite these growing concerns, empirical research on the lived experiences of individuals subject to biometric surveillance remains limited, particularly in non-Western contexts where surveillance practices and regulatory environments may differ substantially. Studies exploring community perceptions, awareness, and the socio-legal implications of biometric technologies are essential to understand the nuanced human rights impacts and inform the development of appropriate policies and safeguards (Kumar & Shah, 2020). This study addresses this gap by conducting a qualitative, community-based investigation into the human rights implications of biometric surveillance in Tehran, a major metropolitan center experiencing increasing biometric technology adoption.

The integration of biometric systems in Iran has advanced rapidly, particularly within public administration, border control, and law enforcement (Rahimi, 2019). However, regulatory frameworks governing biometric data collection, storage, and use remain underdeveloped, raising critical questions about oversight, consent, and accountability (Azadi & Zarei, 2020). Moreover, public understanding of biometric surveillance and its potential risks is often limited, exacerbating fears and mistrust toward government institutions (Karimi & Mohammadi, 2021). This research thus provides valuable insights into how biometric surveillance affects individuals' perceptions of their privacy, autonomy, and rights, contributing empirical evidence from a context less represented in global scholarship.

Privacy concerns dominate discourse surrounding biometric surveillance. According to Solove (2021), privacy is a multifaceted concept encompassing the right to control personal information, freedom from surveillance, and protection against data misuse. Biometric data, due to its unique and immutable nature, poses significant challenges in this regard. Unlike passwords or identification cards, biometric identifiers cannot be changed if compromised, making unauthorized access or breaches particularly harmful (Matsakis, 2019). Several studies have highlighted the vulnerability of biometric databases to hacking and misuse, raising alarms about data security and potential identity theft (O'Flaherty, 2020). Additionally, the psychological impact of constant surveillance, described as "surveillance anxiety," can lead to altered behaviors, reduced civic participation, and self-censorship, thereby diminishing democratic freedoms (Fuchs, 2017; Ball, Haggerty, & Lyon, 2012).

Legal and ethical considerations around biometric surveillance further complicate the human rights landscape. While some jurisdictions have enacted comprehensive data protection regulations, including biometric-specific provisions (e.g., the European Union's General Data Protection Regulation - GDPR), many countries lack clear legislation or enforcement mechanisms to protect individuals (Kuner, 2017). The absence of robust legal safeguards fosters regulatory gaps, allowing authorities and private actors to deploy biometric technologies with limited oversight (Mantelero, 2016). Furthermore, the principle of informed consent is difficult to uphold in contexts where biometric data collection is mandatory for accessing essential services or where refusal may result in exclusion

(Taylor, Floridi, & van der Sloot, 2017). Ethical frameworks emphasize responsible use, transparency, and accountability, yet these principles are frequently neglected in practice, leading to public mistrust and social backlash (Nissenbaum, 2010; Zuboff, 2019).

The social implications of biometric surveillance extend beyond the individual to affect community dynamics and social cohesion. Research has documented instances of discriminatory practices enabled by biometric technologies, including racial profiling, ethnic targeting, and social exclusion (Eubanks, 2018; Benjamin, 2019). In particular, marginalized groups often bear the brunt of surveillance-related harms, which can entrench existing inequalities and stigmatization (Noble, 2018). Community awareness and education about biometric surveillance remain limited, which impedes informed public discourse and the ability to hold authorities accountable (Tufekci, 2015). Conversely, promoting public participation and civic engagement in surveillance policy-making processes is crucial for fostering democratic governance and safeguarding rights (Taylor, 2016).

Technological factors critically shape the human rights impact of biometric surveillance. Accuracy and reliability concerns are paramount, as biometric systems have been shown to produce false positives and negatives that can result in wrongful arrests or denial of services (Grother, Ngan, & Hanaoka, 2019). Data management practices, including retention periods and cross-border data flows, raise questions about control and sovereignty over personal data (Bradshaw, Millard, & Walden, 2011). Furthermore, technological accessibility issues may exclude vulnerable populations, exacerbating digital divides (van Dijk, 2020). Transparency regarding algorithmic processes and integration with other data systems is vital for public trust but often lacking (Diakopoulos, 2016). Striking a balance between technological innovation and human rights protection remains a key challenge for policymakers and society at large (Floridi, 2018).

In light of these concerns, this study seeks to investigate the human rights impact of biometric surveillance through a qualitative approach focusing on the lived experiences and perceptions of community members in Tehran. By employing semi-structured interviews and thematic analysis, the research aims to elucidate privacy concerns, legal and ethical issues, social and community effects, and technological factors as understood by those directly affected. The findings intend to contribute to academic discourse, inform policy development, and advocate for enhanced protections and ethical governance of biometric surveillance.

Methods and Materials

This qualitative study employed a community-based approach to explore the human rights impact of biometric surveillance. Data were collected through semi-structured interviews to obtain in-depth insights from participants regarding their experiences and perceptions. The study sample consisted of 27 individuals residing in Tehran, selected using purposive sampling to ensure diversity in age, gender, occupation, and exposure to biometric surveillance technologies. Recruitment continued until theoretical saturation was reached, whereby no new themes or information emerged from additional interviews.

Semi-structured interviews were conducted using an interview guide developed based on a review of relevant literature and consultation with experts in human rights and surveillance studies. The interviews were conducted face-to-face in Persian, lasted approximately 45 to 60 minutes each, and were audio-recorded with participant consent. Interview questions explored participants' awareness, experiences, concerns, and perceived human rights implications related to biometric surveillance in their communities.

All interviews were transcribed verbatim and imported into NVivo software for systematic qualitative data analysis. Thematic analysis was conducted following Braun and Clarke's approach, involving initial familiarization with the data, generation of initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the final report. Coding was carried out independently by two researchers to enhance reliability, and discrepancies were resolved through discussion until consensus was reached. The analytical process was iterative and aimed at capturing the nuanced human rights concerns associated with biometric surveillance as experienced by community members.

Findings and Results

Privacy Concerns

Participants expressed significant concerns regarding privacy, which was captured through several subthemes. First, Data Collection Awareness revealed a widespread lack of informed consent and transparency about the scope and purpose of biometric data collection. One participant stated, "I had no idea my fingerprints were being stored or how they might be used later" (P12). Relatedly, Data Security Risks emerged as a critical worry, with participants fearing hacking incidents and unauthorized access to their sensitive biometric information. As one interviewee noted, "Who protects this data? What if hackers get it and misuse it?" (P5). The emotional toll of surveillance was evident in the subtheme Surveillance Anxiety, where individuals reported feeling constantly watched, leading to stress and paranoia. For example, a participant shared, "It feels like there's always a camera tracking my every move; it's exhausting" (P19). This anxiety impacted participants' everyday routines (Impact on Daily Life), as some avoided public places or censored their behaviors due to fear of being monitored. Trust in institutions managing these systems was low, with many citing Distrust in Authorities: "I don't trust the government to keep my data safe or use it fairly" (P8).

Legal and Ethical Issues

Legal and ethical challenges surfaced prominently across the participant narratives. The subtheme Human Rights Violations included concerns about infringements on privacy, freedom, and potential discriminatory practices such as profiling. A participant emphasized, "Biometric surveillance can be used to unfairly target minorities; that's a real violation of rights" (P3). Participants also pointed to significant Regulatory Gaps — the lack of clear laws and enforcement mechanisms left many feeling vulnerable: "There's no real law that stops them from doing whatever they want with our data" (P14). Issues surrounding Consent and Autonomy were troubling; many felt coerced into participation without meaningful choice, as one interviewee remarked, "It's not really consent when refusing means losing access to services" (P22). The demand for Ethical Use of Technology underscored participants' calls for accountability and responsible practices: "Surveillance should have strict ethical guidelines to prevent abuse" (P7).

Social and Community Impact

The social repercussions of biometric surveillance were highlighted in various subthemes. Discrimination and Bias was frequently mentioned, with participants reporting experiences and fears of racial profiling and social exclusion. A participant noted, "I worry these systems target people like me unfairly because of my ethnicity" (P16). The community's general Awareness and Education about biometric technologies was limited, resulting in misinformation and fear, as expressed by a participant: "Most people don't understand how these systems work or their rights" (P24). Social Cohesion suffered as trust eroded, leading to community fragmentation and heightened tensions: "People don't trust each other anymore, and this technology only makes it worse" (P10). Vulnerable

groups such as the elderly, refugees, and disabled persons faced disproportionate challenges (Impact on Vulnerable Groups), with one participant emphasizing, "For refugees like me, surveillance feels like constant suspicion" (P1). Nonetheless, some participants saw potential in Public Participation efforts to improve transparency and accountability: "If the community has a say, maybe these systems could be fairer" (P26). Cultural attitudes also influenced acceptance, with Cultural Perceptions varying widely; a participant observed, "Some communities see surveillance as normal, others reject it outright" (P21).

Technological Factors

Participants identified several technological dimensions affecting their experiences with biometric surveillance. Accuracy and Reliability concerns were common, including fears of false positives and system errors that could lead to wrongful consequences: "If the system makes a mistake, it could ruin someone's life" (P9). How data was handled was also a major issue under Data Management, with calls for clear retention policies and anonymization: "Our data shouldn't be kept forever or shared without our permission" (P4). Technological Accessibility emerged as a barrier, with some participants excluded due to lack of access or digital literacy: "Not everyone can use these systems properly, which leaves many behind" (P15). The degree of Integration with Other Systems raised alarms about data being used beyond intended purposes, such as by law enforcement or commercial entities: "My biometric data is probably linked to many databases I don't even know about" (P20). Participants emphasized the importance of User Control over Data, including rights to access, correct, or delete their information: "We should be able to control our own data, not just hand it over" (P11). Calls for Technological Transparency focused on making algorithms and processes understandable and auditable: "People deserve to know how decisions are made by these systems" (P18). Finally, participants reflected on the balance between Innovation and Human Rights, advocating for ethical innovation that respects freedoms: "Progress is good, but not at the cost of our basic rights" (P13).

Discussion and Conclusion

This study explored the human rights implications of biometric surveillance from the perspectives of community members in Tehran. The findings revealed four overarching themes—privacy concerns, legal and ethical issues, social and community impact, and technological factors—that together illustrate the complex and multifaceted nature of biometric surveillance's influence on individuals and society.

Privacy concerns were the most prominent theme emerging from participants' narratives. The subthemes of data collection awareness and data security risks highlight a fundamental lack of transparency and perceived vulnerability regarding biometric data handling. Participants reported feeling inadequately informed about how their biometric information was collected, stored, and potentially shared. This aligns with existing literature emphasizing the opacity of biometric systems and the difficulty individuals face in exercising meaningful control over their personal data (De Hert & Papakonstantinou, 2018; Solove, 2021). The anxiety stemming from pervasive surveillance, reflected in the subtheme of surveillance anxiety, is consistent with findings by Fuchs (2017) and Ball, Haggerty, and Lyon (2012), who document the psychological stress and behavioral changes induced by continuous monitoring. Participants' reports of altered behaviors and self-censorship also resonate with broader concerns that surveillance technologies may suppress democratic freedoms and public participation (Tufekci, 2015). Distrust in authorities regarding data protection and ethical use further exacerbates these concerns, echoing Greenleaf's (2018) observations about public skepticism in contexts with weak regulatory frameworks.

The **legal and ethical issues** theme uncovered significant gaps in regulation, consent practices, and ethical governance. Participants perceived a lack of comprehensive legislation and enforcement mechanisms to protect biometric data, which parallels global critiques about insufficient legal safeguards for emerging surveillance technologies (Mantelero, 2016; Kuner, 2017). The difficulty in securing truly informed consent—particularly when participation is effectively mandatory to access essential services—is a critical ethical challenge widely acknowledged in the literature (Taylor, Floridi, & van der Sloot, 2017). This coercion undermines autonomy and contravenes fundamental human rights principles (Nissenbaum, 2010). Calls from participants for responsible and accountable use of biometric technologies echo ethical frameworks that stress transparency, fairness, and accountability in algorithmic decision-making (Diakopoulos, 2016; Zuboff, 2019). These findings reinforce the urgent need to align biometric surveillance deployment with established human rights and ethical standards.

Regarding **social and community impact**, participants described biometric surveillance as a source of discrimination, social exclusion, and erosion of trust. Concerns about profiling and bias reflect well-documented issues with biometric systems exhibiting disparate accuracy across racial and ethnic groups (Buolamwini & Gebru, 2018; Garvie, Bedoya, & Frankle, 2016). Such biases contribute to social marginalization and deepen existing inequalities, consistent with Benjamin's (2019) critique of surveillance as a tool of systemic oppression. Limited community awareness and education about biometric technologies compound these effects, as misinformation and knowledge gaps hinder public debate and democratic oversight (Tufekci, 2015). The fragmentation of social cohesion and heightened tensions within communities resonate with Eubanks' (2018) findings on how surveillance disproportionately harms vulnerable populations, such as minorities, refugees, and disabled persons. However, participants' emphasis on public participation and community engagement in surveillance governance aligns with literature advocating for inclusive policy-making to foster trust and accountability (Taylor, 2016).

Finally, **technological factors**—including accuracy, data management, accessibility, system integration, user control, and transparency—shaped participants' perceptions of biometric surveillance. Concerns about false positives and system errors reflect critical issues documented in multiple evaluations of facial recognition and fingerprint technologies (Grother, Ngan, & Hanaoka, 2019). Erroneous identifications not only threaten individual rights but also undermine public confidence in these systems. Participants' worries about data retention, sharing, and lack of control over their biometric data mirror wider debates on data sovereignty and privacy in the digital age (Bradshaw, Millard, & Walden, 2011). The digital divide and technological accessibility concerns highlighted the risk of excluding disadvantaged groups, consistent with van Dijk's (2020) analysis of digital inequalities. The limited transparency regarding algorithmic decision-making and system integration reported by participants echoes calls for explainability and auditability in AI and biometric technologies to ensure fairness and accountability (Diakopoulos, 2016; Floridi, 2018). Balancing technological innovation with human rights protections remains a pressing policy challenge underscored by this study (Zuboff, 2019).

In summary, this research confirms and extends prior studies by providing rich qualitative insights into how biometric surveillance affects human rights perceptions within a specific sociopolitical context. The experiences of Tehran's residents underscore the global relevance of privacy, legal, social, and technological challenges associated with biometric systems. Furthermore, the findings illustrate the interconnectedness of these dimensions, where technological design, legal frameworks, and social contexts jointly shape the impact of surveillance on human rights.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adheried in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

Ball, K., Haggerty, K. D., & Lyon, D. (Eds.). (2012). Routledge handbook of surveillance studies. Routledge.

Benjamin, R. (2019). Race after technology: Abolitionist tools for the new Jim code. Polity Press.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. International Journal of Law and Information Technology, 19(3), 187–223. https://doi.org/10.1093/ijlit/eaq020

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.

De Hert, P., & Papakonstantinou, V. (2018). The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 34(2), 222–235. https://doi.org/10.1016/j.clsr.2017.05.014

Diakopoulos, N. (2016). Accountability in algorithmic decision making. Communications of the ACM, 59(2), 56–62. https://doi.org/10.1145/2844110

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

Floridi, L. (2018). Artificial intelligence, education, and the fourth industrial revolution. Philosophy & Technology, 31(4), 467–479. https://doi.org/10.1007/s13347-018-0311-0

Fuchs, C. (2017). Social media: A critical introduction (2nd ed.). SAGE.

Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws including Indonesia and Turkey. Privacy Laws & Business International Report, (147), 10–13.

Grother, P., Ngan, M., & Hanaoka, K. (2019). Ongoing face recognition vendor test (FRVT), part 2: Identification. NIST Interagency/Internal Report (NISTIR)–8238. National Institute of Standards and Technology.

Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to biometrics. Springer.

Karimi, S., & Mohammadi, A. (2021). Public perception of surveillance technologies: A case study in Tehran. Journal of Iranian Social Studies, 15(2), 45–62.

Kuner, C. (2017). The General Data Protection Regulation: A commentary. Oxford University Press.

Kumar, S., & Shah, S. (2020). Public perceptions of biometric surveillance in emerging economies: A review. Journal of Information Privacy and Security, 16(3), 175–194.

Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.

Mantelero, A. (2016). Personal data for decisional purposes in the age of big data: From an individual to a collective dimension of data protection. Computer Law & Security Review, 32(2), 238–255. https://doi.org/10.1016/j.clsr.2016.02.004

Matsakis, L. (2019). Biometric data is forever. Wired. https://www.wired.com/story/biometric-data-is-forever/

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. NYU Press.

O'Flaherty, K. (2020). Biometric data breaches and risks. Cybersecurity Journal, 12(1), 24–33.

Rahimi, M. (2019). Biometric technologies in Iran: Applications and challenges. Iranian Journal of Technology, 43(4), 213–227.

Solove, D. J. (2021). Understanding privacy (2nd ed.). Harvard University Press.

Taylor, L. (2016). Transparent surveillance: Privacy, consent, and trust. Palgrave Macmillan.

Taylor, L., Floridi, L., & van der Sloot, B. (2017). Group privacy: New challenges of data technologies. Philosophy & Technology, 31(4), 369–374. https://doi.org/10.1007/s13347-017-0261-6

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(203), 203–218.

United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

van Dijk, J. (2020). The digital divide. Polity Press.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.