Oxford Human Rights Hub
A global perspective on human rights

Data Protection Human Dignity Right to Freedom of Association
Right to Freedom of Speech and Expression Right to Privacy India

AI, Surveillance and Privacy in India: Human Rights in the Age of Technology

by Tripti Bhushan | Sep 3, 2025

About Tripti Bhushan

Tripti Bhushan is an *Author* & currently working as Assistant Professor *at O.P Jindal Global Law School and as Fellow at Centre for Law and Humanities at Jindal Global University , Sonipat, Haryana, India . She has also worked as an Assistant Professor at Kalinga University, Raipur. She has completed her undergraduate program (B.A, LL.B) (Hons) from Amity Law School, Lucknow. She further pursued her Post Graduate Program (LL.M) in Intellectual Property Rights from Hidayatullah National Law University, Raipur.* She is also the *recipient of the International Award as Emerging Scientist in the field of law.* She has won *Research Excellence Award at Jindal Global Law School for her excellent contribution in Research & Publication in 2021.* She has also received the *Award for Best External Paper:' in Annual conference organized by Kent Law School, UK (2021).*

Tripti has various publications in journals like *Indonesian Journal of International Law, Economic and Political Weekly (EPW), NTUT Journal of Intellectual Property and Management, Oxford University Hub, Law School Policy Review NLSIU Bangalore, International Journal of Public Law and Policy, UNHRC, Journal of Intellectual Property Rights, and IGI Global.*
Additionally, she has completed various national & international courses from W.I.P.O, CISCO Networking Academy, United States Institute of Peace, Dr. Ram Manohar Lahiya National Law University, Lucknow, The Law Learners, ADBI Institute, University of Geneva, and Amity University, Alison. She has also completed a Professional Development Program from University of Buraimi. She has also completed the IP Awareness / Training Program under National Intellectual Property Awareness Mission (NIPAM) organized by the Intellectual Property Office. Tripti is the Advisory Board Member of International Centre for Intellectual Property Laws (IC-IPL) & Young Member at Young ICCA (International Council for Commercial Arbitration).

In recent years, India has increasingly adopted artificial intelligence (AI) surveillance tools. This includes facial recognition cameras at railway stations and predictive policing software in city police departments. The country's technological ambitions clash with the constitutional rights to privacy, dignity, and freedom. Supporters say that AI improves efficiency and security. However, expanding surveillance infrastructure without strong legal protections poses serious risks to human rights in a nation already facing problems of discrimination, lack of transparency, and poorly regulated law enforcement.

India's Automated Facial Recognition System (AFRS) was launched by the National Crime Records Bureau to help track "missing persons" and identify criminals. But critics argue that the system has been deployed for much broader policing objectives—often disproportionately impacting vulnerable groups. The Delhi Police, for instance, used facial recognition software during the 2020 anti-CAA protests to identify and track protesters. This practice raises pressing concerns under the Indian Constitution, especially Articles 19(1)(a) (freedom of speech and expression) and 21 (protection of life and personal liberty), as affirmed in the landmark *KS Puttaswamy v Union of India* (2017) 10 SCC 1, where the Supreme Court unequivocally recognised the right to privacy as a fundamental right.

Facial recognition not only chills the right to protest and assemble but also carries the risk of algorithmic bias. A report by Internet Freedom Foundation (2023) revealed that facial recognition tools in India suffer from accuracy issues and lack transparency regarding vendor accountability, storage of data, and audit mechanisms. This is particularly worrying in a country with weak data protection infrastructure.

Predictive policing tools—software that anticipates where crimes might occur or who might commit them—have entered India's law enforcement toolkit. States like Uttar Pradesh and Telangana have piloted such technologies, echoing developments in countries like the United States. However, the opacity of these algorithms and their reliance on historically biased data raise red flags. As legal scholar Usha Ramanathan notes, India's criminal databases are often shaped by caste, class, and communal prejudices, leading to over-policing of marginalised communities.

The risk is double: not only could predictive policing perpetuate current social hierarchies, but it also reallocates discretionary authority from the judiciary and police to impenetrable algorithms with no accountability. Without an independent security mechanism or transparent statutory framework governing AI in criminal justice, such tools are at risk of undermining the constitutional presumption of innocence and the due process protections under Article 22.

India's much-awaited data protection regime finally came into being when the Digital Personal Data Protection Act, 2023 (DPDPA) came into force. Nevertheless, the legislation has been derided for favoring state interests at the expense of individual rights. Section 17 of the DPDPA permits the government to exempt any agency of the government from the operation of the act

for purposes as wide as “National Interest”. Moreover, the legislation is devoid of substantive safeguards on surveillance, fails to establish a data protection authority with appropriate autonomy, and provides no practical remedies for breaches of privacy.

Unlike the EU’s General Data Protection Regulation (GDPR), which places strict limitations on data processing by public authorities, India’s framework enables vast discretion to state actors—especially law enforcement agencies—under the guise of public order or national security. This permissiveness undermines the Supreme Court’s direction in *Puttaswamy (Aadhaar)* (2019) 1 SCC 1 that surveillance must meet the tests of legality, necessity, and proportionality.

AI-powered surveillance systems being used across India, with no consideration being given to corresponding rights-based protections, shows a sad drifting away from the constitutional framework. Concerns are growing that new technologies, such as facial recognition and predictive policing, are being implemented without any form of public debate, comment, or even judicial oversight, which could make a culture of surveillance commonplace.

In order to curb the risk of digital authoritarianism, India needs to impose targeted legislation for surveillance, i.e. policing algorithms, enforcing transparency, and enforcing oversight of surveillance systems. Civil society should also campaign for reform of DPDPA to align its provisions with human rights norms, particularly the International Covenant on Civil and Political Rights (ICCPR), of which India is a signatory.

Technology need not be at odds with rights—but only if it is embedded within a democratic and accountable legal framework. India’s digital future depends on getting that balance right.

Data Protection Human Dignity Right to Freedom of Association

Right to Freedom of Speech and Expression Right to Privacy

Share this: