LIVING UNDER THE DIGITAL EYE: HUMAN RIGHTS, PRIVACY, AND JUSTICE IN AN ERA OF GLOBAL SURVEILLANCE

Mrs. Raunak Gupta[1] & Ms. Prerna Singh[2]

ABSTRACT

In the digital world of the globalised world, personal information is now both an asset and a liability in the digital world. As one of the largest digital societies across the globe, India faces certain challenges that are unique to finding the balance between the promotion of technology and the preservation of basic rights. This paper focuses on the impact of domestic and international surveillance practices on justice and privacy with a reference to India.

It discusses the tension between individual and state security, evaluates the recently enacted Digital Personal Data Protection Act, 2023, and reviews such seminal cases as Justice K.S. Puttaswamy v. Union of India (2017). The article justifies stronger security measures, ethical principles, and a humanistic attitude towards digital policies by putting India in the global context of surveillance and human rights.

Keywords: Constitutional Rights, Privacy, Surveillance, DPDP, Privacy.

[1] Assistant Professor, IILM University, Greater Noida (India)
[2] LLM (Criminal Law), IILM University Greater Noida (India)

INTRODUCTION

The twenty-first century has seen the emergence of unprecedented growth of digital societies, in which day-to-day interactions communication, finance, healthcare, governance, and more are mediated by data-based infrastructures.[3] The rise of smartphones, social media, biometrics, artificial intelligence and big-data analytics has changed the way states and non-governmental organisations monitor, index and analyse human behaviour.[4] Surveillance in this setting has become not so much a focused and exceptional state practice but a backgrounded and everyday quality of life. The digital ecosystem is generating data trails that expose intimate information about people, which makes personal information both an asset and a significant weakness at the same time.[5]

Personal information is the asset of national economies, company profit models and administrative regulating models; on the other hand, the abuse of it may result in identity theft, discrimination, profiling and violation of rights.[6] The digital age is a paradox because the same technologies that are intended to make life easier and more secure increase the potential of intrusion, monitoring, and control. This is the tension between technology advancement and personal liberties which is the center of the current world discourse concerning digital privacy, surveillance and human rights.

India can be considered one of the largest and most rapidly developing digital societies in the world, and systems like Aadhaar, DigiLocker, CoWIN, FASTag, and the UPI payment system have become an inseparable part of daily life.[7] These inventions have facilitated effective welfare provision, financial inclusion and administrative convenience. At the same time, they have developed massive databanks holding biometric data, money data, movement data, and data on communications.[8] The Digital Personal Data Protection Act, 2023 (DPDP Act) is the initial effort to regulate the laws of India to set personal data, user rights, and obligations of data fiduciaries in a comprehensive manner.[9] Nonetheless, the Act has received a mixed reception because it has extensive exemptions to government agencies, inadequate oversight

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism* 12–18 (PublicAffairs, 2019).
[4] David Lyon, *Surveillance Studies: An Overview* 21–32 (Polity Press, 2018).
[5] Daniel J. Solove, *Understanding Privacy* 1–5 (Harvard University Press, 2008).
[6] U.N. Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (2014).
[7] Ministry of Electronics and Information Technology (MeitY), *India's Digital India Programme Overview* (2023).
[8] Sriram Bharadwaj, "Aadhaar and the Creation of a Biometric State in India," 57 *Economic & Political Weekly* 45– 50 (2022).
[9] Digital Personal Data Protection Act, No. 22 of 2023 (India).

and lacking strict measures against state surveillance.[10]

The human rights dilemma comes into play here, how do we get India to use digital transformation as a means of development without compromising privacy, dignity, autonomy and the freedom of democracy? Surveillance technologies, including biometric authentication platforms and centralised surveillance systems like the Central Monitoring System (CMS), NATGRID and social-media analytics, are associated with issues of proportionality, transparency, responsibility and misuse. This historic ruling of the Supreme Court in **Justice K.S. Puttaswamy v. Union of India (2017)**, privacy was established as one of the fundamental rights, under Article 21 of the Constitution, to provide a constitutional benchmark against which state surveillance practices could be assessed.[11] However, there is an indication of a disjuncture between constitutional undertakings and realities of operations in the relentless nature of unregulated monitoring mechanisms.

It is on this context that the current study will analyze how human rights, privacy and justice intersect in an era of increasing digital surveillance with keen interest in the emerging legal and technological environment in India. The research problem focuses on the fact that there is no consistent and rights-protective framework that regulates the process of surveillance, even though India is actively developing in the digital field. The purpose of the research is to critically examine the effect of surveillance practices on core rights, assess the sufficiency of the current legislation, in particular, of the DPDP Act, 2023, and place India in the context of the world discourse on the issue of digital governance. The importance of the study is that it contributes to the existing debate on the topic of privacy jurisprudence, the dilemma between national security and civil liberties, and the necessity of ethical, transparent, and human-oriented regulatory frameworks.

The paper is organized structurally into five parts:

- Section 2 gives a conceptual clarity of surveillance and discusses world models.

- Section 3 is on the surveillance ecosystem of India, comprising of legal provisions and the technological infrastructures.

[10] Internet Freedom Foundation, *An Analysis of the Digital Personal Data Protection Act, 2023* (2023).
[11] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

- Section 4 assesses the human rights concerns that modern surveillance practices bring about.

- Section 5 analyses the DPDP Act, 2023 critically and its conformity to the constitutional and international standards.

- Section 6 also ends with suggestions on how to establish a balanced and rights-respecting digital governance framework.

UNDERSTANDING SURVEILLANCE: CONCEPTS, MODELS, AND GLOBAL TRENDS

In its simplest meaning, surveillance can be defined as the systematic gathering, observation and study of data concerning individuals or groups, usually with the aim of governing, security or social control. Mass surveillance refers to the tendencies in which information is gathered without any form of individualized suspicion and in a population-wide manner, usually through automated digital means. As a contrast, specific individuals or entities are targeted under specific grounds in accordance with established standards, e.g. criminal investigations, threats to national security, or compliance with regulations.[12] The transition of monitoring that is based on individuals to ubiquitous tracking of data is one of the characteristic aspects of the digital age.

In the past, surveillance was based on physical observation; human intelligence, policing networks, and records kept manually. Surveillance has now become integrated into the communication systems, financial platforms, biometric databases, social media networks, and algorithmic infrastructures with the development of digital technologies, however,[13] This change has widened the range and invisibility of practices of monitoring. In the case of physical surveillance, which was restrictive to human resources and logistics, digital surveillance is highly fast, high-scale, and automated and frequently without the knowledge or approval of the monitored individuals.[14] This development brings forth serious issues of privacy, autonomy, informational asymmetry, and institutional power concentration to ensure that institutions that

[12] Article 29 Working Party, *Opinion 03/2016 on the Evaluation and Review of the ePrivacy Directive* (2016).
[13] Gary T. Marx, *Windows Into the Soul: Surveillance and Society in an Age of High Technology* 34–41 (University of Chicago Press, 2016).
[14] Alessandro Acquisti, Curtis Taylor & Liad Wagman, "The Economics of Privacy," 54 *Journal of Economic Literature* 442–492 (2016).

regulate enormous data streams.

The theory of surveillance capitalism formulated by Shoshana Zuboff is a critical conceptual framework in this context, whereby Zuboff believes that to predict, influence and capitalize on human behaviour, the private technology corporations collect behavioural data.[15] In contrast to traditional surveillance where state agents play the main role, surveillance capitalism is a business that flourishes on commercial motives, establishing a worldwide exchange of data profiles, targeted advertising, behavioural pushes, and algorithmic manipulation.[16] It is this combination of the capabilities of individual and governmental surveillance that makes accountability more difficult, as states are more and more relying on corporate infrastructures to provide intelligence and data analytics, and corporations are enjoying leeways in accountability and lax regulations.

The global models of surveillance differ greatly in jurisdictions. The U.S. paradigm is featured by the use of intelligence-led operations that are backed by the gathering of data by the private sector, such as the comprehensive surveillance system that was unveiled by the Snowden leaks.[17] Big tech companies including Google, Meta, Amazon, and Apple are at the heart of defining data ecosystems by establishing complicated relationships between national security agencies and business organizations.[18]

European Union model, which is developed based on the General Data Protection Regulation (GDPR), displays a rights-based perspective putting an emphasis on consent, transparency, data minimization, and robust enforcement measures.[19] The focus of human dignity and informational autonomy by the EU has seen GDPR become a reference point on international data protection.

In comparison, the Chinese model is a very state-oriented surveillance system that combines facial recognition networks, biometric surveillance, and the Social Credit System into one

[15] Shoshana Zuboff, *The Age of Surveillance Capitalism* 67–83 (PublicAffairs, 2019).
[16] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* 25–33 (Oxford University Press, 2019).
[17] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* 15–30 (Metropolitan Books, 2014).
[18] Ben Wagner, "The Political Economy of the Internet: Google's Role in State Surveillance," 40 *Telecommunications Policy* 1017–1024 (2016).
[19] General Data Protection Regulation, Regulation (EU) 2016/679, arts. 5–7 (EU).

sociotechnical system.[20] Not only is this model developed to control crime but to manage the social, evaluate behaviour and create political stability, it exemplifies the broadest type of digital state surveillance in the modern world.[21]

These world models are important lessons to India. The surveillance situation in India is changing very fast, but there is no strong rights-based protection as in the EU, or the institutional transparency that should be created in democratic regimes.[22] Meanwhile, the magnitude of digital governance in India reflects some structural characteristics of the U.S. and Chinese models, such as the use of intermediaries of a private nature and the growth of biometric and data-driven systems. [23] In its quest to enhance its digital governance system, India should focus on proportionality, judicial checks and balances, accountability measures, and data protection rules that are citizen-oriented to prevent repeating the dangers of unregulated surveillance systems. Finally, the problem that India faces is the ability to use technological innovation without violating the constitutional values and international human rights principles.[24]

THE INDIAN SURVEILLANCE LANDSCAPE: LAWS, TECHNOLOGIES, AND INSTITUTIONS

The surveillance architecture in India has developed considerably in the last 20 years due to the accelerated digitisation, security concerns of a country, and the development of biometric and datadriven governance structures. The combination of Aadhaar, NATGRID, the Central Monitoring System (CMS), NETRA, and various social-media-monitoring systems create a thick net of systems, which allow collecting data in real-time, checking identities, and intercepting communications.[25] These instruments are used at varying degrees of statutory support, supervision, and visibility among the various state agencies.

The Aadhaar, the largest biometric identity programme in the world, is the basis of many authentication procedures in welfare programmes, banking, tax collection, telecommunication

[20] Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control," 28 *Communications of the ACM* 38–42 (2022).
[21] Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," ASPI Policy Brief (2019).
[22] Vrinda Bhandari & Renuka Sane, "Towards a Privacy Law in India," 52 *Economic & Political Weekly* 1–7 (2017).
[23] Malavika Jayaram, "India's Orwellian State: Biometrics and Beyond," *Carnegie India Report* (2020).
[24] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[25] Malavika Jayaram, "India's Orwellian State: Biometrics and Beyond," *Carnegie India Report* (2020).

and even in the operations of the private sector.[26] Although the idea of Aadhaar was to simplify the welfare provision and cut down on leakages, its involvement with financial dealings, mobile networks, and citizen databases has broadened its role more than what it was initially intended to accomplish.[27] The records of Aadhaar authentication, metadata trails and centralised biometric storage bring in the question of the potential of surveillance particularly in the light of no strong purpose-limitation protection.

The other important element is the National Intelligence grid (NATGRID), which is structured to be an integrated intelligence system that connects airlines, banks, tax systems, immigration systems, and telecom service providers databases to facilitate the identification of the pattern and analysis of threats to be used by the law enforcement agencies.[28] NATGRID is suggested as a counter-terrorism instrument, but the specifics of its operation are in the shadows and the tool does not have a specific legislative framework outlining the powers, restrictions, and accountability frameworks.[29]

Central monitoring system (CMS) is one of the most extensive communication monitoring systems in India. It enables security agencies to intercept phone calls, SMS and internet traffic straight off the telecom networks without necessarily involving the services providers.[30] CMS is not only providing automated and centralised surveillance facilities as opposed to the previous interception systems, which demanded human intervention and monitoring and is of concern, in terms of how well it complies with constitutional protection provisions in Puttaswamy.

To supplement CMS, there is NETRA (Network Traffic Analysis), an intelligence tool created at the Defence Research and Development Organisation (DRDO) to spy on internet traffic, keywords, and other suspicious communication patterns on social media and email platforms.[31] In addition to them, other ministries have social-media observation cells, which monitor the mood on the Internet, detect disinformation, and assess the possible threats to civil order in the country.[32] These surveillance units actively scan user activity, posts, and comments on a regular

[26] Unique Identification Authority of India (UIDAI), *Aadhaar Dashboard* (2023).
[27] Reetika Khera, "Aadhaar as a Medium of Exclusion," 56 *Economic & Political Weekly* 12–15 (2021).
[28] Ministry of Home Affairs, Government of India, *NATGRID Overview* (2022).
[29] Internet Freedom Foundation, *NATGRID and the Absence of Legal Safeguards* (2021).
[30] Centre for Internet and Society (CIS), *India's Surveillance State: CMS Analysis* (2015).
[31] DRDO, *NETRA Project Overview* (2019).
[32] Ministry of Information & Broadcasting, *Social Media Communication Hub Guidelines* (2018).

basis, and this is becoming part of a growing system of digital behavioural surveillance.

The legal system that regulates these systems is disjointed and old-fashioned. The information technology act of 2000 in section 69 gives the government the authority to intercept, monitor and decrypt electronic information due to reasons such as the sovereignty, security and order of the people.[33] The regulations which are set in the context of this section offer procedural protections but have been criticised in not allowing wide executive discretion with no external control.[34] The Telegraph Act 1885 which was initially passed to govern colonial telegraphy still governs interception of telephone conversations though it is no longer compatible with the modern digital technologies.[35] Both these laws precede the establishment of privacy as a fundamental right, and both do not reflect modern requirements of necessity, proportionality or data minimisation.

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the first effort to enact laws on the protection of individual rights to personal data and stipulate the responsibilities of data fiduciaries in India. Although the Act creates the consent presuppositions, grievance opportunities, and responsibilities of data fiduciaries, it also provides broad exemptions to the state to meet the national security, social order, and prevention of crimes.[36] The Act does not place hard restrictions on state surveillance, does not give the interception activities prior judicial approval and does not have algorithmic transparency provisions.[37] Moreover, the new Data Protection Board is not an independent regulatory authority with investigative and enforcement authority, but an adjudicatory body, which restricted its capacity to regulate the practice of government surveillance.[38]

In the past, India did not have an all-encompassing data protection agency, which would regulate the use of personal data by states and the private sector, creating uneven protection, higher risks of data breach, and unregulated growth of surveillance systems.[39] Despite the DPDP Act, issues of the so-called function creep, i.e. the progressive extension of surveillance instruments beyond their intended use, such as the inclusion of Aadhaar in financial and

[33] Information Technology Act, No. 21 of 2000, § 69 (India).
[34] Pranesh Prakash, "The Need for Surveillance Reform in India," 4 *Indian Journal of Law & Technology* 1–17 (2019).
[35] Telegraph Act, No. 13 of 1885 (India).
[36] Digital Personal Data Protection Act, No. 22 of 2023, § 17 (India).
[37] Internet Freedom Foundation, *Analysis of DPDP Act* (2023).
[38] Amber Sinha, "Why the Data Protection Board Is Not a Regulator," *The Hindu* (2023).
[39] Vrinda Bhandari & Renuka Sane, "Towards a Privacy Law in India," 52 *Economic & Political Weekly* 1–7 (2017).

telecommunication services, despite the prohibitive court ruling, are still present.[40] The frequent data breaches of government databases and websites of the public sector also reveal structural vulnerabilities in cybersecurity and accountability to a greater extent.[41]

Compared to the international standards, the Indian framework is inferior to rights-oriented frameworks, including the GDPR of the European Union, that require strict necessity tests, data minimisation, independent regulators and transparency requirements. [42] India does not have significant redress mechanisms to state surveillance, unlike in the United States where the surveillance of the populace is dominated by the private-sector, but limited by litigation and industry legislation. Equally, although the surveillance systems in China are blatantly state-led, in India, the model has a danger of becoming broad in scope with no clear statutory basis, procedural protection, and democracy restraints that can otherwise govern abuse.

As an Indian, there is a need to implement more robust schemes of judicial review, legislative transparency, audit systems and transparency in the hands of the people so that the technological innovation cannot harm constitutional liberties. In the absence of these protections, the surveillance environment will grow unregulated at the expense of privacy, autonomy, and even democratic accountability.[43]

HUMAN RIGHTS IMPLICATIONS: PRIVACY, LIBERTY, EQUALITY, AND JUSTICE

The high rate of growth of digital surveillance in India has both direct and far-reaching consequences on human rights, especially, the right to privacy, liberty, equality and access to justice. Privacy, which is identified as a fundamental right in **justice K.S. Puttaswamy (Retd.) v. Union of India**, is the constitutional framework on which the contemporary criticism of surveillance is based.[44] The Court believed that privacy safeguards not just the autonomy and dignity of the person, but also decisional freedom, control over information and the right against unreasonable state intrusion.[45] The digital surveillance systems, in turn, can be implemented without proper transparency, control, or proportionality, which poses a threat of

[40] Udbhav Tiwari, "Function Creep in India's Digital Systems," *Observer Research Foundation Issue Brief* (2020).
[41] CERT-In, *Annual Cyber Security Report* (2022).
[42] General Data Protection Regulation, Regulation (EU) 2016/679.
[43] Anja Kovacs, *The Internet and Freedom in India* (Internet Democracy Project, 2021).
[44] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[45] Gautam Bhatia, *Privacy and the Constitution of India* 47–58 (Oxford University Press 2019).

the constitutional right to privacy being compromised in reality.

One of the human rights issues is the chilling effect caused by ubiquitous surveillance. When people are aware or even have some suspicions that their online actions, interactions, or behavioural patterns are monitored, they might avoid voicing their dissenting views, discussing politics, or otherwise being involved in civil society.[46] This chilling effect is not a hypothetical one: it has been recorded that online activism was lower, and so was the desire to participate in a democratic dialogue in a highly surveilled setting, as it has been in studies.[47] To the journalists, activists, and minority groups, the intimidation of being monitored can prompt them not to report, legislate or mobilise the community, thus, reducing civic space.

The case of the Pegasus spyware in India shows the pressing nature of targeted online surveillance. The claims that journalists, human-rights activists, opposition politicians and lawyers were monitored with the help of sophisticated spyware was an indication that digital intrusion equipment can be used to undermine professional secrecy, dissent, and democratic accountability. This kind of surveillance may corrupt the criminal justice system by putting at stake the principle of equality before the law, which is against Articles 14 and 21 of the Constitution.[48]

The other significant issue is that of algorithmic discrimination, which has been caused by automated decision-making processes that are integrated in policing, welfare checks, financial risk ratings, and face recognition. Algorithms based on surveillance can be biased or may exert negative influences on pre-existing social biases, disadvantaging marginalised communities, including Dalits, Muslims, migrants, and the poor (Hoffman 2019). Facial recognition tools have been proven to be more prone to errors with a darker skin color and among women in international studies, which casts doubts on the accuracy and fairness of their implementation in the Indian public space.[49] Algorithms surveillance is a threat to strengthen the social inequalities and facilitate the structural injustice without transparency, audit mechanisms, or anti-discrimination safeguards.

[46] David Cole & Federico Fabbrini, "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders," 14 *International Journal of Constitutional Law* 220–245 (2016).
[47] Pen America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (2013).
[48] Article 14 & 21, Constitution of India.
[49] Inioluwa Deborah Raji et al., "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results," 2019 *AAAI/ACM Conference on AI Ethics* 429–439.

Another issue with digital surveillance is the integrity of the criminal justice system. The growing popularity of predictive policing systems, metadata analysis, and surveillance of communication increases the ability of investigative organizations, but it can also open the gate to misuse, false profiling, or manipulation of evidence to fit the desired outcome.[50] Without legal restrictions, judicial checks, and balances, surveillance-based evidence may lead to infringement of rights to a fair trial, the attorney-client privilege, and the creation of imbalances between state authority and personal rights, as well as undermine the attorney-client privilege and result in unequal treatment of the state and the individual (Davies and Prusak, 2018).

In addition to state surveillance, corporate actors have an important role in influencing surveillance ecosystems by tracking their behaviours, target advertising and monetising their information. Such erosion of boundaries between the surveillance of the state and the surveillance of the individual makes it harder to hold anyone accountable and also makes it harder to have control over personal information.[51] Social media captures enormous quantities of data about users, including their location, browsing history, biometrics, and can be provided to state agencies with wide exemptions under the law.[52] These risks are compounded by the broad exemptions of the government in the DPDP Act which focuses on national-security and public-order goals without creating independent checks and a right to notification.[53]

Of great importance is the effect of surveillance in democratic participation. The conformity and punishment of dissent are valued by the surveillance settings, which compromise the deliberative nature of democracy.[54] Constant tracking of online behaviour, including scanning of social media, sentiment analysis, and profiling, can inform political messaging, voter behaviour, and strategies of micro-targeting that corrupt the electoral process.[55] These practices pose a danger to the values of free speech, informed choice and equal political participation.

Finally, the principle of uncontrolled surveillance is a threat to the fundamental constitutional principles of dignity, autonomy, equality and justice. India needs to enhance the protection of democratic integrity by introducing proportionality standards, judicial authorisation, legislative clarity, and algorithmic accountability measures. In the absence of such safeguards, the

[50] Rashida Richardson, "Dirty Data, Bad Predictions," 94 *New York University Law Review* 192–238 (2019).
[51] Shoshana Zuboff, *The Age of Surveillance Capitalism* 115–127 (PublicAffairs 2019).
[52] Facebook v. Union of India, (2019) 9 S.C.C. 349 (India).
[53] Internet Freedom Foundation, *Analysis of DPDP Act* (2023).
[54] Anja Kovacs, *The Internet and Freedom in India* (Internet Democracy Project, 2021).
[55] U.N. Special Rapporteur on Freedom of Expression, *Surveillance and Democracy*, U.N. Doc. A/76/258 (2021).

growing surveillance machine will lead to the shift of the relationship between the state and the citizen to the one of suspicion, fear, and unequal power, which will change the nature of the constitutional democracy in India.

THE IMPACT OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), is the first detailed law in India regulating the rights to personal data and the data-processing responsibilities. The Act is a major move in the changing digital governance in India, trying to find solutions to the issues that are raised due to the high volumes of personal data produced by biometric systems, financial solutions, welfare programmes, and online services. Nevertheless, being as it is, the DPDP Act casts enormous doubts regarding whether it can be an effective protection against unregulated surveillance.

The architecture of the Act is constructed on three main pillars which include consent, data fiduciaries duties, and data principal rights. Consent, according to the Act, should be specific, informed and should be free will, where people should be allowed to revoke whenever they want to do so. The data principals are given the right to information concerning their data, request correction or erasure, and appoint a representative to act on their behalf.[56] Data fiduciaries must maintain reasonable security measures, address complaints and must report breaches of data to the Data Protection Board.[57] These provisions indicate a move to be in line with the international best practices which have focused on the agency of individual and transparency in data processing.

Although these improvements have been made, the Act has wide exemptions of government agencies, which greatly weaken its protective power. Section 17 allows the Central Government to dispense any state instrumentality of compliance with consent, purpose-limitation, or dataminimisation requirement based on national security, sovereignty, social order, or offence prevention reasons.[58] These exceptions cannot be judicially reviewed and do not come with necessary and proportionality tests, which gives rise to expansive state surveillance.[59] The DPDP Act grants the executive discretion unlike the GDPR of the European Union, which limits the ability to claim exemptions based on the circumstances by creating

[56] DPDP Act, §§ 12–14.
[57] DPDP Act, §§ 8–10.
[58] DPDP Act, § 17.
[59] Internet Freedom Foundation, *Analysis of DPDP Act* (2023).

limited protection and administrative checks and balances on the executive branch to protect individuals (Berry and Ferrell, 2017).

The other significant issue is related to the Data Protection Board that is not a regulatory authority but mainly an adjudicatory one. The Board does not have the investigative independence, financial independence and enforcement authority that defines robust data protection regulating bodies around the world.[60] This organizational vulnerability casts uncertainty regarding its ability to hold to account potent state agencies or giant technology corporations, particularly the cases pertaining to surveillance practices.[61] The lack of a prior-notification is also a factor that does not allow a person to know whether their data has been processed or accessed by state authorities.

The Act also does not mention the concern of algorithmic transparency and decision-making without human intervention as more and more artificial intelligence is applied to welfare verification, policing, credit scoring, and digital profiling, among others[62]. Lacking policies that would require auditing of fairness, transparency disclosures, and non-discrimination protections, algorithmic systems are likely to continue giving rise to biases and making it possible to conduct opaque surveillance processes that disadvantage vulnerable populations in a unequal way.[63]

The other constraint is related to the cross-border data flows. Although the Act permits the government to limit the transfer of the information to specific jurisdictions, the Act does not outline the protection that should be granted to data that is transferred to foreign surveillance agencies or commercial entities, as well as does not indicate the circumstances in which such transfers can be banned or authorized. This ambiguity poses some risks when it comes to international intelligencesharing agreements, international tech platforms, and international data processing.

Civil society groups have also expressed more concerns about the lack of robust data breach notification schedules, the lack of remedies in the event of an individual, and the possibility of

[60] Amber Sinha, "Why the Data Protection Board Is Not a Regulator," *The Hindu* (2023).
[61] Vrinda Bhandari, "India's Data Protection Law and the Risk of Executive Overreach," *EPW Engage* (2023).
[62] U.N. Special Rapporteur on Privacy, *Report on Artificial Intelligence and Privacy*, U.N. Doc. A/73/438 (2018).
[63] Joy Buolamwini & Timnit Gebru, "Gender Shades," 81 *Proceedings of Machine Learning Research* 1–15 (2018).

function creep, especially with Aadhaar and other digital identity systems.[64] Since India has just witnessed the massive data breaches in the recent past, such as the government portal, welfare databases, and telecom provider leaks, the DPDP Act seems to rely on broad executive powers, with no protection of informational privacy.[65]

The Act does not meet the international human-rights standards, e.g. the UN Guiding Principles on Business and Human Rights, OECD Privacy Guidelines and the jurisprudence of the European Court of Human Rights, in terms of proportionality, independent oversight, and effective remedies.[66] The problem facing India is not simply passing a law on data protection, but that its enforcement does not justify or further empower the surveillance machinery of the state.

As it stands, the DPDP Act offers a valuable basis in which to control personal data in India. But, its effectiveness in protecting basic rights is constrained by the broad exemptions, lax regulatory protection and absence of transparency mechanisms. To be in line with the constitutional provisions expressed in Puttaswamy and other global best practices, India must present stricter measures, rules of judicial oversight and institutional restructurings that make sure that the safeguarding of data is not being used as a cover to increase digital surveillance.[67]

CONCLUSION AND RECOMMENDATIONS

Efficiency, inclusion, and administrative reform possibilities have been opened up by the emergence of digital governance in India, but this has also created a new era of surveillance and data extraction and informational vulnerability. With personal data coming to the fore in the welfare delivery, financial systems, identity checking, and national security, the lines between development and intrusion have become further unclear. The surveillance ecosystem of India, which is based on such technologies as Aadhaar, CMS, NATGRID, NETRA, and social-media monitoring, now functions on an unprecedented large scale. As much as these infrastructures are expected to increase security and administrative capacity, their growth has valid concerns relating to privacy, autonomy, equality, and democratic accountability.

The Digital Personal Data Protection Act, 2023 offers some preliminary concept of personal

[64] Centre for Internet and Society, *Critical Review of India's Data Protection Bill* (2022).
[65] CERT-In, *Cyber Security Annual Report* (2022).
[66] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).
[67] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

data protection but is not sufficient to create a full-scale protection against state abuse. The wide exemptions on the part of the government, the absence of an autonomous regulatory body, and the lack of transparency mechanisms undermine the capacity of the Act to become a true guardian of the basic rights. Meanwhile, the trends in the world, including the rights-focused model of the GDPR, as well as the invasive digital governance of more authoritarian governments, indicate that the course which India will pursue will have a crucial impact on the future of the democratic institutions of the country.

A rights-protective surveillance should be based on the constitutional values, especially dignity, privacy, liberty, and equality. India needs a number of reforms that are urgently needed to get in line with the international standards and respect the principles that have been set in the great constitutional jurisprudence.

To start with, any process involving surveillance has to have judicial oversight as its core. The interception, monitoring, and access request of data should be required to have independent authorisation as opposed to executive discretion. This would make sure that the surveillance is only utilized where it is required and reasonable.

Second, the current adjudicatory model of Data Protection Board should be substituted with a stronger regulatory body, which has investigative powers, autonomy and resources. This regulator should be able to audit both the government and the private bodies, give binding orders and make them obey.

Third, mechanisms of transparency are needed. Regular reports made to the public, audit trail of surveillance orders and a need to inform people except under some restricted circumstances would increase accountability, without undermining national security.

Fourth, India needs to have algorithmic accountability measures. With artificial intelligence integrated into policing, welfare decisions, and digital profiling, the law should impose fairness audits, non-discriminatory protection, and the opportunity to appeal a decision made by the robot.

Fifth, the minimisation of data and limitation of the purpose must be implemented strictly. The use of surveillance systems should not be extended beyond the purpose of their creation and any additional use of the data must be rigidly tested. The issue of functional creep, especially

in the Aadhaar-linked services, should be regulated by explicit legal bans.

Lastly, it is important to involve the masses and consult the people. The surveillance reform is impossible without civil society, academic researchers, journalists, and technical experts. Participatory approach would make sure that the reforms are based on the technological reality and needs of the society.

In conclusion, India is currently at a very dangerous crossroad, where the development of digital governance should be moderated against the constitutional liberties. The unchecked surveillance will lead to the development of an asymmetrical power relationship and constant monitoring between the citizen and the state. India can embrace the opportunities presented by digital technology by employing a rights-based regulatory approach that is human-centred and can protect the primary principles of its democracy. The future is not about struggling against the technological advancement but about making sure that the development of technologies makes the values that the free and just society is founded on even more robust.

Bibliography

Books

- Acquisti, Alessandro, Curtis Taylor & Liad Wagman, The Economics of Privacy, 54 Journal of Economic Literature 442–492 (2016).
- Bhatia, Gautam, Privacy and the Constitution of India (Oxford University Press 2019).
- Cohen, Julie E., Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press 2019).
- Greenwald, Glenn, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (Metropolitan Books 2014).
- Lyon, David, Surveillance Studies: An Overview (Polity Press 2018).
- Marx, Gary T., Windows Into the Soul: Surveillance and Society in an Age of High Technology (University of Chicago Press 2016).
- Solove, Daniel J., Understanding Privacy (Harvard University Press 2008).
- Zuboff, Shoshana, The Age of Surveillance Capitalism (PublicAffairs 2019).

Journal Articles

- Bharadwaj, Sriram, Aadhaar and the Creation of a Biometric State in India, 57 Economic & Political Weekly 45 (2022).
- Bhandari, Vrinda & Renuka Sane, Towards a Privacy Law in India, 52 Economic & Political Weekly 1 (2017).
- Bhatia, Gautam, Privacy and Constitutionalism in India, Oxford University Press (2019).
- Cole, David & Federico Fabbrini, Bridging the Transatlantic Divide?, 14 International Journal of Constitutional Law 220 (2016).
- Creemers, Rogier, China's Social Credit System, 28 Communications of the ACM 38 (2022).
- Jayaram, Malavika, India's Orwellian State: Biometrics and Beyond, Carnegie India (2020).
- Khera, Reetika, Aadhaar as a Medium of Exclusion, 56 Economic & Political Weekly 12 (2021).
- Prakash, Pranesh, The Need for Surveillance Reform in India, 4 Indian Journal of Law &

Technology 1 (2019).

- Richardson, Rashida, Dirty Data, Bad Predictions, 94 New York University Law Review 192 (2019).
- Wagner, Ben, The Political Economy of the Internet, 40 Telecommunications Policy 1017 (2016).

Reports, Policy Papers & Institutional Publications

- Amber Sinha, Why the Data Protection Board Is Not a Regulator, The Hindu (2023).
- Anja Kovacs, The Internet and Freedom in India (Internet Democracy Project 2021).
- Centre for Internet and Society, India's Surveillance State: CMS Analysis (2015).
- Centre for Internet and Society, Critical Review of India's Data Protection Bill (2022).
- CERT-In, Annual Cyber Security Report (2022).
- Hoffman, Samantha, Engineering Global Consent, ASPI Policy Brief (2019).
- Internet Freedom Foundation, Analysis of the Digital Personal Data Protection Act (2023).
- Internet Freedom Foundation, NATGRID and the Absence of Legal Safeguards (2021).
- Ministry of Electronics and Information Technology, Digital India Programme Overview (2023).
- Ministry of Home Affairs, NATGRID Overview (2022).
- OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).
- Pen America, Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor (2013).
- UIDAI, Aadhaar Dashboard (2023).

International & UN Documents

- Article 29 Working Party, Opinion 03/2016 on the ePrivacy Directive (2016).
- General Data Protection Regulation, Regulation (EU) 2016/679.
- U.N. Human Rights Council, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37

(2014).

- U.N. Special Rapporteur on Privacy, Artificial Intelligence and Privacy, U.N. Doc. A/73/438 (2018).

- U.N. Special Rapporteur on Freedom of Expression, Surveillance and Democracy, U.N. Doc. A/76/258 (2021).

Indian Statutes

- Constitution of India, arts. 14 & 21.

- Digital Personal Data Protection Act, No. 22 of 2023.

- Information Technology Act, No. 21 of 2000.

- Telegraph Act, No. 13 of 1885.

Cases

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

- Facebook Inc. v. Union of India, (2019) 9 S.C.C. 349 (India).