SURVEILLANCE TECHNOLOGY AND DATA PROTECTION: A COMPARATIVE CONSTITUTIONAL ANALYSIS OF INDIA AND CHINA IN THE DIGITAL AGE

Indira Chakraborty, Shyambazar Law College affiliated with the University of Calcutta.

ABSTRACT:

The proliferation of surveillance technologies in the digital era presents profound challenges to the constitutional fabric of democratic societies, necessitating a delicate equilibrium between national security imperatives and fundamental privacy rights. This article undertakes a comprehensive comparative analysis of surveillance regimes in India and China, examining the constitutional, statutory, and regulatory frameworks governing digital surveillance and data protection. Through doctrinal analysis and comparative methodology, this study evaluates the Digital Personal Data Protection Act, 2023, in India against China's tripartite data governance structure comprising the Cybersecurity Law, Data Security Law, and Personal Information Protection Law. The research reveals significant constitutional divergences in approaching surveillance technology governance, with India's rights-based framework contrasting sharply with China's state-centric surveillance apparatus. The analysis demonstrates that while both jurisdictions grapple with technological advancement and security concerns, their constitutional foundations and implementation mechanisms differ substantively, creating distinct implications for individual liberty, democratic governance, and the rule of law. The article concludes with recommendations for strengthening India's surveillance governance framework while preserving constitutional values and democratic principles.

Keywords: Surveillance Technology, Data Protection, Constitutional Law, Privacy Rights, Comparative Law, Digital Governance

I. Introduction

The digital revolution has fundamentally transformed the relationship between state power and individual liberty, creating unprecedented opportunities for surveillance while simultaneously challenging traditional constitutional frameworks designed to protect privacy and personal autonomy.[1] In this evolving landscape, the regulation of surveillance technology has emerged as one of the most pressing constitutional questions of our time, requiring careful calibration between legitimate security interests and fundamental rights.[2]

The constitutional significance of surveillance regulation extends beyond mere policy considerations to encompass fundamental questions about the nature of democratic governance, the scope of state power, and the protection of human dignity in the digital age.[3] As Justice D.Y. Chandrachud observed in the landmark *Puttaswamy* decision, "Privacy is not a mere policy choice for legislative majorities to make; it is a constitutional value which straddles across the spectrum of rights."[4]

This article examines the constitutional and legal frameworks governing surveillance technology in India and China, two populous nations with fundamentally different approaches to individual rights and state power.[5] The comparative analysis reveals not merely differences in regulatory approach, but fundamental divergences in constitutional philosophy, democratic governance, and the conceptualisation of individual liberty in the digital era.

The significance of this comparative study is underscored by the recent enactment of India's Digital Personal Data Protection Act, 2023 (DPDP Act), which represents a pivotal moment in India's data protection jurisprudence.[6] Simultaneously, China's comprehensive surveillance architecture, encompassing the Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021), provides a contrasting model of state-centric data governance.[7]

---

[1] See SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 8-12 (2019).
[2] Julie E. Cohen, What Privacy is For, 126 HARV. L. REV. 1904, 1905 (2013).
[3] Neil Richards, The Dangers of Surveillance, 126 HARV. L. REV. 1934, 1935-40 (2013).
[4] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1, ¶ 180.
[5] See generally ORVILLE SCHELL & JOHN DELURY, WEALTH AND POWER: CHINA'S LONG MARCH TO THE TWENTY-FIRST CENTURY (2013).
[6] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (2023).
[7] See generally ROGIER CREEMERS, CHINA'S SOCIAL CREDIT SYSTEM: AN EVOLVING PRACTICE OF CONTROL (2018).

II. Theoretical Framework and Literature Review

A. Constitutional Theory and Surveillance Power

The theoretical foundation for analysing surveillance technology regulation rests upon constitutional theory concerning the relationship between state power and individual liberty. [8] Classical liberal theory, as articulated by Mill and subsequent constitutional scholars, emphasises the presumptive liberty of individuals against state interference, requiring compelling justification for any limitation of personal freedom.[9]

In the context of surveillance technology, this theoretical framework demands rigorous scrutiny of state surveillance powers, ensuring they are exercised within constitutional bounds and subject to meaningful oversight.[10] The German Federal Constitutional Court's conception of "informational self-determination" provides a particularly influential theoretical foundation, recognising individual autonomy over personal information as fundamental to human dignity and democratic participation.[11]

B. Comparative Constitutional Analysis

Comparative constitutional methodology enables systematic examination of how different legal systems approach similar challenges while remaining sensitive to contextual differences in constitutional culture, political structure, and historical development.[12] The comparison between India and China is particularly instructive given their shared challenges of technological advancement, security concerns, and population scale, while maintaining fundamentally different constitutional foundations.[13]

C. Digital Rights Theory

The emergence of digital rights theory recognises that traditional constitutional rights require reinterpretation and application in the digital context.[14] Privacy, in particular, has evolved from

[8] See ISAIAH BERLIN, FOUR ESSAYS ON LIBERTY 118-72 (1969).
[9] JOHN STUART MILL, ON LIBERTY 13-14 (1859).
[10] See generally DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE (2001).
[11] BVerfGE 65, 1 (1983) (F.R.G.).
[12] See RAN HIRSCHL, COMPARATIVE MATTERS: THE RENAISSANCE OF COMPARATIVE CONSTITUTIONAL LAW 2-3 (2014).
[13] See PRATAP BHANU MEHTA, THE BURDEN OF DEMOCRACY 1-15 (2003).
[14] See JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 1-8 (2019).

Warren and Brandeis's "right to be let alone" to encompass complex questions of data governance, algorithmic decision-making, and digital surveillance.[15]

Contemporary scholars have identified several dimensions of digital privacy: informational privacy (control over personal data), communications privacy (protection of electronic communications), and behavioural privacy (freedom from monitoring and profiling).[16] Each dimension raises distinct constitutional questions and requires different regulatory approaches.

III. Constitutional Foundations: India's Rights-Based Framework

A. The Puttaswamy Revolution

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* fundamentally transformed India's constitutional landscape by recognising privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution.[17] This nine-judge bench decision explicitly overruled earlier precedents that had denied constitutional protection to privacy, establishing a robust foundation for challenging state surveillance powers.[18]

Justice Chandrachud's lead judgment articulated a comprehensive theory of privacy encompassing three dimensions: "repose (freedom from unwanted stimuli), sanctuary (protection of the inner self), and intimate decision (autonomy over fundamental personal choices)."[19] This tripartite conception provides a sophisticated framework for analysing surveillance technology's impact on constitutional rights.

The Court's recognition of privacy as a fundamental right carries significant implications for surveillance regulation. Any limitation of privacy rights must satisfy the strict scrutiny test of legality, necessity, and proportionality.[20] This constitutional standard requires that surveillance measures be authorised by law, pursue legitimate aims, and employ means proportionate to their objectives.[21]

---

[15] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 193 (1890).
[16] See DANIEL SOLOVE, UNDERSTANDING PRIVACY 1-15 (2008).
[17] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.
[18] The decision overruled M.P. Sharma v. Satish Chandra, AIR 1954 SC 300, and Kharak Singh v. State of U.P., AIR 1963 SC 1295.
[19] Puttaswamy, (2017) 10 SCC 1, ¶ 183.
[20] Id. ¶ 181.
[21] Id.

B. Article 21 and Surveillance Technology

The incorporation of privacy within Article 21's guarantee of life and personal liberty creates a presumption against state surveillance activities that cannot be justified by compelling public interest.[22] This constitutional foundation requires careful examination of any surveillance program to ensure compliance with constitutional standards.

The Supreme Court's emphasis on procedural due process in *Maneka Gandhi v. Union of India* further strengthens protections against arbitrary surveillance.[23] The Court's insistence that any procedure established by law must be fair, just, and reasonable provides additional safeguards against excessive surveillance powers.[24]

C. Fundamental Rights and State Power

The constitutional tension between individual rights and state power is particularly acute in the surveillance context. While the Constitution recognises the state's legitimate security interests, it establishes clear boundaries on the exercise of such power.[25] The doctrine of proportionality, developed through judicial interpretation, provides a framework for balancing competing interests while preserving constitutional values.[26]

IV. India's Digital Personal Data Protection Act, 2023: A Critical Analysis

A. Legislative Framework and Scope

The Digital Personal Data Protection Act, 2023, represents India's first comprehensive data protection legislation, establishing a rights-based framework for regulating personal data processing.[27] The Act's scope extends to all digital personal data processing within India and outside India in connection with any business carried on in India or any systematic activity of offering goods or services to data principals in India.[28]

---

[22] INDIA CONST. art. 21.
[23] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[24] Id. ¶ 7.
[25] See UPENDRA BAXI, THE FUTURE OF HUMAN RIGHTS 89-92 (3d ed. 2008).
[26] See AHARON BARAK, PROPORTIONALITY: CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS 3-8 (2012).
[27] Digital Personal Data Protection Act, 2023, § 1.
[28] Id. § 3.

The Act defines personal data broadly as "data about an individual who is identifiable by or in relation to such data," encompassing various forms of digital information that can identify natural persons.[29] This broad definition ensures comprehensive protection while raising questions about the Act's interaction with existing surveillance frameworks.

B. Data Principal Rights and State Surveillance

The DPDP Act establishes several fundamental rights for data principals, including rights to information, correction, erasure, and grievance redressal.[30] However, the Act's interaction with state surveillance activities remains complex and potentially problematic.

Section 17 of the Act provides significant exemptions for government processing in the interests of sovereignty, integrity, security of the state, public order, or preventing cognizable offences.[31] These broad exemptions potentially undermine the Act's protective framework by creating expansive exceptions for government surveillance activities.

The exemption provisions raise constitutional concerns given their breadth and lack of specific safeguards. Unlike the European Union's General Data Protection Regulation, which requires that exemptions be necessary and proportionate, the DPDP Act's exemptions appear to grant broader discretion to government authorities.[32]

C. Enforcement Mechanism and Data Protection Board

The Act establishes a Data Protection Board of India with extensive powers to investigate violations, impose penalties, and issue directions.[33] The Board's independence is crucial for effective enforcement, though questions remain about its relationship with government surveillance agencies.

The penalty structure under the Act includes fines up to ₹250 crores for significant data fiduciaries, demonstrating the legislature's commitment to enforcement.[34] However, the

[29] Id. § 2(t).
[30] Id. §§ 11-14.
[31] Id. § 17.
[32] Regulation (EU) 2016/679, art. 23, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[33] Digital Personal Data Protection Act, 2023, § 18.
[34] Id. § 33.

exemption of government processing from many penalty provisions raises questions about accountability in state surveillance activities.

V. China's Surveillance State: Legal Architecture and Implementation

A. The Tripartite Framework

China's approach to surveillance regulation operates through a comprehensive legal framework comprising three principal statutes: the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (2021).[35] This tripartite structure reflects China's systematic approach to digital governance while prioritising state security and social stability.[36]

The Cybersecurity Law establishes the foundation for China's digital governance regime, emphasising network security and data localisation requirements.[37] The law grants extensive powers to government authorities for network monitoring and data access, reflecting China's security-centric approach to digital governance.[38]

B. Social Credit System and Surveillance Integration

China's Social Credit System represents perhaps the most comprehensive surveillance apparatus in contemporary history, integrating various data sources to create comprehensive profiles of individuals and organisations.[39] The system's legal foundation rests upon the broader framework of digital governance laws while extending surveillance capabilities far beyond traditional law enforcement contexts.[40]

The integration of social credit mechanisms with surveillance technology creates a system of

[35] See generally GRAHAM WEBSTER, ROGER CREEMERS & PAUL TRIOLO, FULL TRANSLATION: CHINA'S CYBERSECURITY LAW (2017).
[36] JOSH CHIN & LIZA LIN, SURVEILLANCE STATE: INSIDE CHINA'S QUEST TO LAUNCH A NEW ERA OF SOCIAL CONTROL 15-18 (2022).
[37] Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017).
[38] Id. arts. 21-23.
[39] See JEREMY DAUM, THE CHINA PROJECT, CHINA'S SOCIAL CREDIT SYSTEM IN 2021: FROM FRAGMENTATION TOWARDS INTEGRATION (2022).
[40] State Council Notice Concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020), CHINA COPYRIGHT & MEDIA (June 14, 2014).

pervasive monitoring that fundamentally alters the relationship between state and citizen.[41] Unlike traditional surveillance systems focused on specific security threats, the social credit system creates comprehensive behavioural monitoring with significant implications for social and economic participation.[42]

C. Data Localisation and State Control

China's data governance framework emphasises strict data localisation requirements, mandating that certain categories of data be stored within China's borders.[43] These requirements serve both security and surveillance purposes, ensuring government access to data while limiting foreign surveillance capabilities.[44]

The Data Security Law's classification of data into categories ranging from general to core national data creates a hierarchical system prioritising state security over individual privacy.[45] This approach reflects China's constitutional emphasis on collective welfare and state security over individual rights.[46]

VI. Comparative Constitutional Analysis: Rights Versus Security

A. Constitutional Foundations and State Power

The fundamental constitutional difference between India's and China's approach to surveillance technology stems from their divergent constitutional foundations. India's Constitution, grounded in liberal democratic principles, establishes individual rights as fundamental limitations on state power.[47] The recognition of privacy as a fundamental right creates a presumption against state surveillance that must be overcome through compelling justification.[48]

---

[41] See MAJA DARUWALA, THE SURVEILLANCE STATE: BIG DATA, FREEDOM AND YOU 45-52 (2019).
[42] Id.
[43] Data Security Law of the People's Republic of China, arts. 19-24 (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021).
[44] Id.
[45] Id. art. 21.
[46] XIAN. art. 51 (1982) (China).
[47] INDIA CONST. arts. 14-32.
[48] Puttaswamy, (2017) 10 SCC 1, ¶ 181.

China's constitutional framework, by contrast, emphasises the primacy of state power and collective welfare over individual rights.[49] The Chinese Constitution's emphasis on state security and social stability provides broad justification for surveillance activities that would face constitutional challenges in India's rights-based system.[50]

B. Judicial Review and Accountability

The availability of meaningful judicial review represents a crucial difference between the two systems. India's constitutional framework provides robust judicial review of government action, including surveillance activities, through fundamental rights litigation.[51] The Supreme Court's willingness to scrutinise government surveillance programs, as demonstrated in cases involving privacy rights, provides meaningful accountability mechanisms.[52]

China's system, while including formal legal protections, provides limited opportunity for judicial challenge to government surveillance activities.[53] The party-state structure and emphasis on political stability over individual rights create a system where surveillance activities face minimal independent oversight.[54]

C. Technological Governance and Democratic Values

The relationship between technological governance and democratic values differs fundamentally between the two systems. India's approach, despite its limitations, maintains democratic principles of transparency, accountability, and individual rights as constraints on surveillance technology deployment.[55] The DPDP Act's emphasis on consent, purpose limitation, and data subject rights reflects these democratic values.[56]

China's technological governance model prioritises efficiency and social control over democratic participation and individual autonomy.[57] The integration of surveillance technology

[49] XIAN. pmbl. (1982) (China).
[50] Id. art. 51.
[51] INDIA CONST. art. 32.
[52] See, e.g., Puttaswamy, (2017) 10 SCC 1.
[53] See generally BENJAMIN L. LIEBMAN, THE CHINA QUARTERLY, CHINA'S COURTS: RESTRICTED REFORM (2007).
[54] Id.
[55] See GRANVILLE AUSTIN, THE INDIAN CONSTITUTION: CORNERSTONE OF A NATION 50-75 (1966).
[56] Digital Personal Data Protection Act, 2023, §§ 5-7.
[57] See REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 32-38 (2012).

with social management systems creates a model of technological authoritarianism that fundamentally alters the nature of citizenship and political participation.[58]

VII. Ethical Implications and Constitutional Concerns

A. Privacy and Human Dignity

The deployment of surveillance technology raises fundamental questions about human dignity and the nature of constitutional personhood.[59] As surveillance capabilities expand, the capacity for comprehensive monitoring of individual behaviour creates risks to the autonomous development of personality that constitutional privacy rights are designed to protect.[60]

The chilling effect of pervasive surveillance on democratic participation represents a particular concern for constitutional democracy.[61] When citizens reasonably fear comprehensive monitoring of their activities, their willingness to engage in political dissent, association, and expression may be substantially diminished, undermining the democratic process itself.[62]

B. Algorithmic Governance and Constitutional Rights

The increasing reliance on algorithmic decision-making in surveillance systems creates new constitutional challenges.[63] Automated surveillance systems may perpetuate and amplify existing biases while making decisions affecting fundamental rights with limited human oversight.[64]

The opacity of algorithmic surveillance systems creates particular challenges for constitutional accountability.[65] When surveillance decisions are made by complex algorithms, it becomes difficult for individuals to understand the basis for such decisions or to challenge them

[58] Id.
[59] See JÜRGEN HABERMAS, BETWEEN FACTS AND NORMS: CONTRIBUTIONS TO A DISCOURSE THEORY OF LAW AND DEMOCRACY 99-103 (1996).
[60] Id.
[61] See FREDERICK SCHAUER, FEAR, RISK AND THE FIRST AMENDMENT: UNRAVELING THE CHILLING EFFECT, 58 B.U. L. REV. 685, 686-90 (1978).
[62] Id.
[63] See CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 3-8 (2016).
[64] Id.
[65] See FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3-7 (2015).

effectively through legal processes.[66]

C. Democratic Governance and Technological Power

The concentration of surveillance capabilities in state institutions raises broader questions about the relationship between technological power and democratic governance.[67] As surveillance technology becomes more sophisticated and pervasive, it may alter the fundamental balance of power between government and citizens in ways that undermine democratic accountability.[68]

The international dimension of surveillance technology, particularly the development and deployment of surveillance systems by authoritarian regimes, creates additional challenges for democratic governance.[69] The export of surveillance technology from China to other countries raises questions about the global implications of different approaches to surveillance governance.[70]

VIII. Recommendations and Reform Proposals

A. Strengthening India's Surveillance Governance Framework

India's surveillance governance framework requires significant strengthening to address constitutional concerns while maintaining legitimate security capabilities. The following recommendations emerge from this comparative analysis:

First, the DPDP Act's exemption provisions require substantial revision to ensure compliance with constitutional standards of necessity and proportionality.[71] The current exemptions are overly broad and lack adequate safeguards against abuse.[72] A reformed framework should require specific justification for surveillance activities and provide meaningful oversight

[66] Id.
[67] See LANGDON WINNER, AUTONOMOUS TECHNOLOGY: TECHNICS-OUT-OF-CONTROL AS A THEME IN POLITICAL THOUGHT 1-12 (1977).
[68] Id.
[69] See SHEENA CHESTNUT GREITENS, SURVEILLANCE STATE: INSIDE CHINA'S QUEST TO LAUNCH A NEW ERA OF SOCIAL CONTROL, 92 FOREIGN AFF. 178 (2013).
[70] Id.
[71] Digital Personal Data Protection Act, 2023, § 17.
[72] Id.

mechanisms.[73]

Second, India needs comprehensive surveillance legislation that establishes clear legal standards for government surveillance activities.[74] The current patchwork of laws governing surveillance creates uncertainty and inadequate protection for constitutional rights.[75] New legislation should establish warrant requirements, judicial oversight, and clear limitations on surveillance powers.[76]

Third, the Data Protection Board requires structural independence and adequate resources to effectively oversee government surveillance activities.[77] The Board's current structure may compromise its ability to challenge government surveillance programs effectively.[78]

B. International Cooperation and Standard Setting

India should actively participate in international efforts to establish norms and standards for surveillance technology governance.[79] The development of international frameworks for surveillance governance can help prevent a "race to the bottom" in privacy protection while maintaining security cooperation.[80]

The export control of surveillance technology represents another area requiring attention. [81] India should establish robust export controls on surveillance technology to prevent its use in human rights violations while supporting legitimate security cooperation.[82]

C. Technological Design and Rights Protection

The integration of privacy-by-design principles into surveillance technology development represents a crucial reform opportunity.[83] Surveillance systems should be designed with built-

[73] See European Court of Human Rights, Roman Zakharov v. Russia, App. No. 47143/06, ¶¶ 232-301 (Dec. 4, 2015).
[74] See PRIVACY INT'L, STATE OF PRIVACY INDIA: SURVEILLANCE LEGAL FRAMEWORK (2018).
[75] Id.
[76] Id.
[77] Digital Personal Data Protection Act, 2023, § 18.
[78] Id.
[79] See G.A. Res. 68/167, ¶ 4 (Dec. 18, 2013).
[80] Id.
[81] See PRIVACY INT'L, THE GLOBAL SURVEILLANCE INDUSTRY 15-18 (2016).
[82] Id.
[83] See ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 1-5 (2009).

in protections for constitutional rights rather than treating privacy as an afterthought.[84]

The development of technological safeguards, including encryption, anonymisation, and access controls, can help ensure that surveillance technology is used consistently with constitutional requirements.[85] These technical measures should be complemented by legal requirements and oversight mechanisms.[86]

IX. Conclusion

This comparative analysis reveals fundamental differences in how India and China approach surveillance technology governance, reflecting deeper constitutional and philosophical divergences about the relationship between state power and individual liberty. India's rights-based constitutional framework provides a foundation for protecting individual privacy and democratic values, though significant challenges remain in implementation and enforcement.

The contrast with China's state-centric surveillance apparatus illuminates both the strengths and weaknesses of India's approach. While India's constitutional protections provide meaningful constraints on surveillance power, the practical implementation of these protections requires continued attention and reform. The DPDP Act represents an important step forward, but substantial work remains to create a comprehensive framework that adequately protects constitutional rights while maintaining legitimate security capabilities.

The ethical implications of surveillance technology extend beyond national boundaries, creating global challenges that require coordinated responses. As surveillance technology becomes increasingly sophisticated and pervasive, the need for robust constitutional protections and democratic oversight becomes ever more urgent. India's experience in balancing security needs with constitutional rights provides valuable lessons for other democracies grappling with similar challenges.

The path forward requires continued vigilance in protecting constitutional values while adapting to technological change. This includes strengthening legal frameworks, ensuring independent oversight, and maintaining democratic accountability for surveillance activities.

[84] Id.
[85] Id.
[86] Id.

Only through such comprehensive reforms can India maintain its commitment to constitutional democracy while effectively addressing the security challenges of the digital age.

The comparative analysis undertaken in this article demonstrates that the choice between security and liberty represents a false dichotomy. Effective surveillance governance requires both robust security capabilities and strong constitutional protections, implemented through democratic institutions and subject to meaningful oversight. India's constitutional framework provides the foundation for achieving this balance, but realising this potential requires continued commitment to constitutional values and democratic governance in the digital age.