



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## BALANCING ELECTION LAWS AND PRIVACY RIGHTS IN INDIA

~ Vaishnavi Upadhyay

### ABSTRACT

*With the growing economy and developing ideas of people, introduction of new technology has laid down the pattern that is exploiting the basic structure of human kind. The evolution of technology in our day to day life has balanced comfort with digital tools. There is wider question that has risen that whether digital tools helps to maintain law and order in society or exploit the privacy of individual's by doing mass surveillance. For the protection of individual different laws have been introduced. This paper examines the importance of 'Right to Privacy' and its significance in election.*

*The ongoing legal analysis that has been introduced in the data collection for the public at large even without their knowing has made the curtain for the citizens. In a country where **Article 21**<sup>1</sup> refers as 'heart' of fundamental rights, During the election period the transparency is not visible and all the powers even the location, GPS tracking is all in the power of Election Commission of India. Under the amended Information Technology Rules, 2026.*

*Subsequently the question has been raised in the landmark precedent like **Justice K.S. Puttaswamy v. Union of India**.<sup>2</sup> Where the importance of privacy was laid down as a fundamental right, and it must be protected at any cost, however proportionality test was introduced. If State action infringes the privacy right's then they must align with the "proportionality test".*

### INTRODUCTION

---

<sup>1</sup> India Const. arts. 21.

<sup>2</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; AIR 2017 SC 4161.

Privacy is not just about keeping secrets. It is about having a space in which you can think, disagree, and choose without someone watching over your shoulder.

When that space is invaded, whether by a corporation mining your data or a government running surveillance programmes, something essential to personhood is damaged. In a democracy, this damage is especially serious because voting is supposed to be a free act, made by an individual who has access to honest information and faces no pressure or manipulation.

India has had a troubled relationship with surveillance and privacy. For decades after independence, courts held that privacy was not even a fundamental right, a position that was finally corrected in 2017 when a nine-judge constitutional bench unanimously recognised privacy as an intrinsic part of life and liberty under Article 21. That judgment, *Puttaswamy*, changed everything. It gave citizens a constitutional weapon to resist arbitrary data collection and forced lawmakers to think more carefully about the boundaries of permissible surveillance.

But recognition of a right and its effective enforcement are two different things. The years since *Puttaswamy* have shown that the government is willing to use digital tools extensively during elections, tracking misinformation, profiling voters, and monitoring political communication, all in the name of protecting electoral integrity. Whether these measures genuinely protect democracy or quietly undermine it is the central question this paper tries to answer.

## CONSTITUTIONAL FRAMEWORK: THE THREE PILLARS

The Indian Constitution does not use the word ‘privacy’ anywhere. And yet, it is now settled law that privacy is fundamental, derived from the combined reading of Articles 14, 19, and 21<sup>3</sup>. Understanding how each of these provisions operates in the election context is important.

### **Article 21, The Right to Life and Personal Liberty**

Article 21 says that no person shall be deprived of their life or personal liberty except according to procedure established by law. This seems narrow, but the Supreme Court has read it broadly. In *Francis Coralie Mullin v. Union Territory of Delhi* (1981), the Court held that Article 21 includes the right to live with dignity. In ***Maneka Gandhi v. Union of India* (1978)**<sup>4</sup>, it held that even a law depriving a person of life or liberty must be fair, just, and reasonable not arbitrary.

---

<sup>3</sup> India Const. arts. 14, 19 & 21.

<sup>4</sup> *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248; AIR 1978 SC 597.

Puttaswamy built on these cases. The judgment held that privacy is a natural extension of the right to life because a person cannot truly live, cannot think, love, dissent, or believe, without a protected sphere of inner life. Justice D.Y. Chandrachud, writing for himself and three others, explained that privacy includes the right to control information about oneself. In the election context, this means a voter has the right to decide who gets to know their political preferences, their location, and their online behaviour. Political targeting that bypasses this consent directly violates Article 21.

### **Article 19(1)(a) <sup>5</sup>Freedom of Speech and Expression**

The right to free speech is foundational to democracy. You cannot have meaningful elections without the ability to criticise the government, debate policy, and form and share opinions without fear. The Supreme Court has repeatedly confirmed that political speech occupies the highest pedestal under Article 19(1)(a).

But AI driven microtargeting does not suppress your speech. It does something subtler and in some ways more damaging, it controls what information you receive.

The Supreme Court recognised in **Secretary, Ministry of Information and Broadcasting v. Cricket Association of Bengal (1995)** <sup>6</sup>that Article 19(1)(a) includes not just the right to speak but also the right of the public to receive information. When platforms and political parties manipulate what information reaches a voter, they infringe this right.

### **Article 14, Equality and Non-Arbitrariness**

Article 14 guarantees equality before the law and equal protection of laws. In *E.P. Royappa v. State of Tamil Nadu* (1974), <sup>7</sup>the Supreme Court held that Article 14 also protects against arbitrariness. Any state action that is arbitrary, that is, random, unreasonable, or without rational basis, violates Article 14.

In the digital election context, Article 14 becomes relevant when algorithms discriminate in ways that have no legitimate basis. If an AI system delivers different political content to voters based on religion, caste, or income, amplifying communal messages to some groups and suppressing them for others, this is both arbitrary and constitutionally suspect. It creates an unequal information environment where different citizens effectively participate in different elections.

---

<sup>5</sup> India Const. arts. 19(a).

<sup>6</sup> *Secretary, Ministry of Information & Broad. v. Cricket Association of Bengal*, (1995) 2 SCC 161.

<sup>7</sup> *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3.

## **STATUTORY FRAMEWORK AND ITS GAPS**

India has several laws that bear on privacy and elections, but they were mostly designed for a world that no longer exists. The result is a legal patchwork that leaves citizens exposed in several important ways.

### **The Representation of the People Act, 1951<sup>8</sup>**

The RPA is the backbone of Indian election law. It governs voter registration, election schedules, candidate qualifications, and electoral offences. Section 123<sup>9</sup> lists ‘corrupt practices’ that can invalidate an election, bribery, undue influence, false statements about candidates, and so on. But the Act was written in 1951. It has no provisions dealing with data harvesting, algorithmic targeting, deepfakes, or AI generated. When a political party uses a detailed psychological profile of a voter to craft a personalised message designed to exploit their fears, the RPA has nothing to say about it.

The Model Code of Conduct issued by the Election Commission of India is also largely silent on digital surveillance. The ECI has issued some advisories on social media conduct, but these are voluntary guidelines, not enforceable law. A political party that violates them faces, at most, a strongly worded letter.

### **The Information Technology Act, 2000 and the 2026 Amendments**

The Information Technology Act, 2000<sup>10</sup> was India’s first attempt at regulating cyberspace. Section 66A, which criminalised ‘offensive’ online speech, was struck down in *Shreya Singhal v. Union of India* (2015)<sup>11</sup> as unconstitutional. Section 69 allows the government to intercept, monitor, and decrypt digital communications in the interest of national security, public order, or sovereignty.

The amended Information Technology Rules, 2026 expanded the scope of permissible surveillance during election periods. They give the Election Commission of India significant powers to access user data from social media platforms, track GPS locations of campaign vehicles, and monitor digital communication for electoral misinformation. These are sweeping powers. The Rules do not require judicial authorisation before surveillance begins. They do not

---

<sup>8</sup> Representation of the People Act, No. 43 of 1951, (India).

<sup>9</sup> Representation of the People Act, No. 43 of 1951, section 123 (India).

<sup>10</sup> Information Technology Act, No. 21 of 2000, (India).

<sup>11</sup> *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

specify the duration for which collected data can be retained. And they do not provide a meaningful remedy for citizens who are wrongly monitored.

This is a serious problem. The Puttaswamy judgment was explicit: any restriction on privacy must be backed by law, must serve a legitimate aim, and must be proportionate. Rules that allow mass data collection without judicial oversight, without a defined purpose limitation, and without individual notification struggle to meet this standard.

### **The Digital Personal Data Protection Act, 2023**

India finally enacted a comprehensive data protection law in 2023. The DPDPA<sup>12</sup> requires data fiduciaries, that is, anyone who collects and processes personal data, to obtain meaningful consent, specify the purpose of data collection, and ensure that data is not used for purposes beyond what was disclosed. It establishes the Data Protection Board of India to handle complaints.

However, the DPDPA contains a significant exemption: it allows the central government to exempt any government agency from the Act's requirements in the interest of state security or public order. This is the same language that has historically been used to justify surveillance without accountability. If election related data collection by the ECI or by intelligence agencies can be exempted from DPDPA requirements, the law's protection effectively disappears at precisely the moment voters need it most.

There is also a gap in the DPDPA's coverage of political parties. Political parties in India are not classified as 'data fiduciaries' under the Act, which means that the detailed voter profiling they conduct, using data obtained from Aadhaar seeding, social media scraping, and commercial data brokers, falls outside the law's reach entirely.

### **THE PROPORTIONALITY TEST AND CURRENT PRACTICES**

The Puttaswamy judgment did not hold that privacy is absolute. It held that restrictions on privacy must satisfy a three parts test: legality and proportionality. This test is now the constitutional standard for evaluating all state action that affects privacy.

Applying this test to current election related surveillance reveals several problems.

On legality: many surveillance practices during elections operate under executive orders, ECI advisories, or broadly worded statutory provisions rather than specific, clearly defined laws.

---

<sup>12</sup> Digital Personal Data Protection Act, No. 22 of 2023 (India).

The 2026 IT Rules <sup>13</sup>expand surveillance powers significantly without amending the parent IT Act through Parliament. This is legally doubtful. A fundamental right can only be restricted by a law passed by Parliament, not by a rule made by the executive under a delegated power.

On legitimate aim: the government's stated objectives, preventing electoral violence, stopping disinformation, ensuring compliance with campaign finance rules, are clearly legitimate. But the connection between those objectives and specific surveillance measures is not always transparent. If the ECI monitors private WhatsApp messages in the name of detecting deepfakes, the connection between the measure and the aim needs to be demonstrated, not assumed.

On proportionality: this is where current practices fail most obviously. Proportionality requires that the state use the least intrusive means available to achieve its aim. Mass surveillance of digital communications during election periods fails this test because less intrusive alternatives exist, for example, targeted investigation of specific complaints, mandatory platform reporting obligations, or an independent electoral cybersecurity agency with judicial oversight. The state's preference for broad, opaque surveillance over narrow, accountable tools cannot be justified under Puttaswamy.

## COMPARATIVE ANALYSIS

India is not the first country to deal with these tensions, and looking at how other democracies have responded is useful.

The European Union's General Data Protection Regulation (GDPR), which came into force in 2018, treats political data as 'special category' data, meaning it can only be processed with explicit consent and strict safeguards. Under GDPR Article 9<sup>14</sup>, information about a person's political opinions is given the same protection as health data and sexual orientation. Several EU member states have gone further: Germany and France have imposed specific prohibitions on psychographic profiling for electoral purposes.

---

<sup>13</sup> Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021, as amended by Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Amendment Rules, 2026 (India).

<sup>14</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 9, 2016 O.J.

In the United Kingdom, the Information Commissioner's Office (ICO) <sup>15</sup>conducted a detailed investigation of political microtargeting after the Brexit referendum. It found that multiple political campaigns had used personal data in ways that violated the Data Protection Act. The ICO levied fines and issued enforcement notices. More importantly, it published a detailed code of practice for the use of data in political campaigns, a document that India currently lacks entirely.

The United States has a different constitutional tradition: the First Amendment's protection of political speech is extremely broad, which makes regulating political advertising difficult. But even in the US, the Federal Election Commission has proposed rules on AI generated political advertisements, and several states have passed laws specifically targeting deepfakes in election campaigns.

Canada amended its Canada Elections Act in 2019 <sup>16</sup>to require digital platforms to maintain a public registry of all political advertisements, including who paid for them and which audience segments they were targeted at. This transparency requirement does not prevent microtargeting, but it ensures that it can be scrutinised and challenged.

India's approach lags behind all of these comparators. The DPDPA does not treat political data as a special category. The ECI has no mandatory transparency regime for digital political advertising. The IT Rules give the government surveillance powers without judicial oversight. If India is serious about protecting both elections and privacy, there is much to learn from these experiences.

## **DEALING WITH THE CHALLENGES**

The problem this paper has described is not unsolvable. What is needed is not less technology, but more accountable technology, systems that serve democratic goals without secretly undermining democratic freedoms. Several specific measures deserve attention.

Firstly, political parties must be brought within the ambit of data protection law. The DPDPA's exemption of political parties from its coverage is indefensible. If a private company that collects your shopping habits must have your consent, a political party that builds a

---

<sup>15</sup> Data Protection Act 2018, c. 12 (U.K.); Information Commissioner's Office, Code of Practice: Political Campaigning (2021).

<sup>16</sup> Canada Elections Act, R.S.C. 2000, c. 9, as amended by Bill C-76, 2019 S.C., c. 31 (Can.).

psychological profile of you must certainly also need it. Parliament should amend the DPDPA to expressly cover political parties and their data process. Election surveillance must be subject to prior judicial oversight. The current framework allows the government to monitor digital communications during elections based on executive authorisation. This is constitutionally inadequate after Puttaswamy. Any surveillance measure that involves accessing private communications, whether of individuals or groups, should require a judicial warrant or, at minimum, a review by an independent oversight body with the power to reject unlawful authorisations.

Secondly, the ECI should establish a mandatory public registry of political advertisements, along the lines of the Canadian model. Every political advertisement published on a digital platform during an election period should be publicly disclosed, along with information about who funded it, which audience segments it targeted, and what data was used. This transparency would allow journalists, researchers, and civil society to hold campaigns accountable without requiring state surveillance.

Lastly, the DPDPA's broad national security exemption needs to be tightened. A blanket exemption that allows the government to bypass data protection obligations 'in the interest of public order' during elections is incompatible with the Puttaswamy framework. Any exemption should be narrowly defined, time limited, and subject to independent review.

## **CONCLUSION**

Privacy and democracy are not enemies. They are, in fact, deeply connected. The secret ballot, the foundation of every modern election, is itself a privacy protection. It exists because the founders of democratic systems understood that a vote made under observation is not truly free. What is true of the ballot box is equally true of the digital spaces in which political opinion is formed today India has come a long way since the days when privacy was not even recognised as a fundamental right. The Puttaswamy judgment of 2017 was a genuine constitutional milestone. But milestones are meaningless if the road beyond them leads nowhere.

The years since Puttaswamy have seen surveillance expand, data protection law lag behind practice, and election campaigns exploit personal data in ways that the judgment clearly prohibits in principle but that have not yet been effectively prohibited in practice.

The argument of this paper is simple: elections must be fair not just in the counting of votes but in the formation of preferences. If the information environment in which citizens make their political choices is corrupted by manipulation, profiling, and targeted disinformation, or



if citizens fear that their political views are being monitored by the state, then the election may be procedurally clean but substantively hollow. Real democracy requires both free elections and free minds. Protecting one without the other is not enough. The constitutional tools already exist. The Puttaswamy proportionality test is capable of striking down overreaching surveillance. What is missing is the political will to apply it consistently, the legislative urgency to fill the gaps in existing law, and the institutional courage of the courts to hold governments accountable when they use the machinery of elections to watch, profile, and nudge the very citizens they are supposed to serve.

## REFERENCE

- 1) Shyam Divan and Arghya Sengupta, *Privacy in India* (Eastern Book Company, 2022).
- 2) Usha Ramanathan, 'A Unique Identity Bill' (2010) 45(21) *Economic and Political Weekly* 10.
- 3) Anja Kovacs, 'Surveillance and the Indian State after Puttaswamy' (2019) 11(1) *Journal of Law, Technology and Policy* 45.
- 4) Election Commission of India, *Guidelines on Social Media and Elections*.
- 5) Information Commissioner's Office (UK), *Investigation into the Use of Data Analytics in Political Campaigns*.
- 6) Law Commission of India, Report No. 272: *Free Speech and Elections* (Ministry of Law and Justice, 2023).