International Journal of Engineering Research and Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 21, Issue 11 (November 2025), PP 41-44

Privacy, Surveillance, and the State: Constitutional Challenges in India's Cybersecurity Regime

VISHVESWARAN. P
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
"SCHOOL OF LAW"

Privacy, Surveillance, and the State: Constitutional Challenges in India's Cybersecurity Regime
VISHVESWARAN. P

Abstract
The growing use of digital technology in government and daily life has made it harder for India to balance protecting national security with preserving people's privacy. This project looks at how India's cybersecurity policies affect the country's constitution, especially the conflict between government surveillance and the right to privacy. It checks how laws like the Information Technology Act, 2000, and later rules, influence the constitutional rights in Articles 14, 19, and 21
The study also examines whether India's cybersecurity laws meet the legal standards of fairness, necessity, and reasonableness set in the Supreme Court case Justice K.S. Puttaswamy v. Union of India (2017). By analyzing laws, court decisions, and how agencies handle cybersecurity, the project finds issues with how accountable, transparent, and properly checked these surveillance practices are. It then suggests ways to improve cybersecurity laws, so they are both strong and upheld the constitution, protecting digital independence while still respecting individual rights.

Date of Submission: 01-11-2025 Date of acceptance: 08-11-2025

I. Introduction & Historical Background of the Topic

The rise of the digital age has changed the way governments use power, gather information, and keep people safe. As digital systems become more important for national security, it is harder to tell where government monitoring ends India's work on cybersecurity, especially through the Information Technology Act, 2000, and its later changes, shows a stronger focus on government control and watching what people do online. In the past, Indian courts did not see privacy as a basic right. Cases like M.P. Sharma v. Satish Chandra (1954)[1] and Kharak Singh v. State of U.P. (1962)[2] said there was no right to privacy. But many years later, in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[3], a Supreme Court judges changed that and said privacy is part of life and freedom under Article 21. This momentous change happened at the same time as India was trying to build strong cybersecurity systems to fight cybercrime, terrorism, and spying. So now there is a problem: how can the government protect digital systems without hurting people's privacy? This project investigates that issue by studying how privacy, government watching, and cybersecurity rules connect in India.

Aims of the Study

1. To examine the constitutional foundations of the right to privacy and their relevance in the context of cybersecurity.
2. To analyze the statutory framework governing cybersecurity and state surveillance in India.
3. To evaluate whether India's cybersecurity policies conform to constitutional principles such as legality, necessity, and proportionality.
4. To identify gaps in judicial and legislative oversight of surveillance mechanisms.
5. To propose policy and legal reforms ensuring that cybersecurity measures respect fundamental rights while supporting national security.

Scope of the Study

[1] *M.P. Sharma v. Sathish Chandra, AIR 1954 SC 300*
[2] *Kharak Singh V. State of U.P., AIR 1963 SC 1295.*
[3] *Justice K.S. Puttaswamy(Retd.) V. Union of India, (2017) 10 SCC 1.*

The study focuses on India's constitutional and legal framework regulating cybersecurity and surveillance. It examines key legislations and instruments including:

- The Information Technology Act, 2000 (especially Sections 69, 69A, and 70B).
- The Indian Telegraph Act, 1885 (interception powers).
- The CERT-In Directions (2022).
- The Digital Personal Data Protection Act, 2023.

The temporal scope extends primarily from 2017 (post-Puttaswamy) to 2025, capturing recent judicial and policy developments. The study excludes purely technical aspects of cybersecurity, focusing instead on constitutional and administrative dimensions.

II. Survey and Review of Literature

After the Puttaswamy case, discussions about privacy and surveillance in India have grown a lot. Scholars like Justice B.N. Srikrishna[4] and Lawrence Laing[5] have debated the limits of state surveillance within a democratic constitutional , The report called the Srikrishna Committee Report (2018) focuses on protecting data but does not talk much about how the government uses cybersecurity to monitor people. Studies from think tanks like ORF and Carnegie India show that there is not enough clear laws or responsibility in India's cybersecurity organisations. Comparing India with places like the European Union, where rules like GDPR and NIS2 are in place, shows that India's focus is more on security than on protecting rights. The main issue in research is looking at how India's cybersecurity policies fit with the country's constitution. Most studies talk about privacy or data protection, but few check if cybersecurity actions follow important legal ideas like fairness and proportionality. This project tries to cover that missing part.

Content of the Project Report

Evolution of the Right to Privacy

Privacy being a constitutional right is one of the most significant changes in Indian law. At first, privacy was considered part of Article 21, which protects the right to life and personal freedom. But in 2017, the Supreme Court made it clear that privacy is a fundamental right in the case Justice K.S. Puttaswamy (Retd.) v. Union of India. A group of nine Hon'ble Supreme Court judges all agreed that privacy is intricately connected to dignity, independence, and freedom. The Court also set out three rules to check if a government action that affects privacy is allowed. These rules are the action must be legal, it must have a good reason, and it must not be more restrictive than needed to reach that goal.

Judicial Interventions and Limitations

Despite the clear guidance from the Puttaswamy case, state surveillance in India still mostly happens under secret executive control. In the case of Anuradha Bhasin v. Union of India (2020)[6], the Hon'ble Supreme Court said having internet access is important for freedom of expression and business. They said internet shutdowns need to be fair and reasonable, but they did not fully stop long or too much control, showing they are not ready to challenge security reasons. In another case, Manohar Lal Sharma v. Union of India (2021)[7]—known as the Pegasus spyware case—the Court admitted that there were serious issues with illegal surveillance of people, especially journalists and activists. Instead of holding the government accountable, they set up a technical group to investigate the matter, without directly criticizing the executive's actions. These cases show that although the courts have said privacy is a key part of the Constitution, they have been careful and not strict when it comes to enforcing privacy in cases related to surveillance and government power**.**

Absence of a Comprehensive Surveillance Framework

India does not have a specific and complete law for surveillance. Different intelligence and law enforcement agencies use interception and monitoring powers through orders from the executive branch and lower-level rules. This scattered and executive-focused system gives wide-ranging decision-making power without any check from a separate court. There is no clear legal limit or single approval process, which creates a

[4] *Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians 1(2018).*

[5] *Lawrence Liang, "Surveillance, Privacy and Constitutionalism in India," Economic and Political Weekly, Vol. 53, No. 40 (2018).*

[6] *Anuradha Bhasin V. Union of India(2020) 3 SCC 637.*

[7] *Manohar Lal Sharma V. Union of India (Pegasus Case), (2021) 10 SCC 1.*

big gap in the legal system. Even though the Constitution protects the right to privacy, there is no proper system in place to ensure this protection.

India's Cybersecurity Legal Architecture

The Information Technology Act, 2000

India's cybersecurity system is based on the Information Technology Act, 2000 (IT Act)[8], which was first made to support e-commerce and digital identity. Over the years, this law has become the main rule for managing digital rules, cybersecurity, and government monitoring. Section 69 allows the government to listen in, watch, or break into digital messages if it thinks it's for national security, country's independence, or public safety. Section 69A lets the government stop people from accessing certain online content, which is often used to block websites, social media, or news sites. Section 70B creates CERT-In, which is the main team in India that deals with cybersecurity issues. While these rules let the government step in during digital matters, they are written in a general way and don't have clear rules about how to handle them. Orders to listen in can be made by high-level officials under the 2009 rules and are checked by groups made only of government workers. There's no need for a judge's approval, outside checking, or public sharing of how decisions are made, which weakens the fairness and accountability of the process.

The CERT-In Directions of 2022

In 2022, CERT (COMPUTER EMERGENCY RESPONSE TEAM)-In issued directions that increased the government's ability to check online activities. These rules ask internet service providers, VPN companies, and data centers to keep user information for five years and to report any security issues quickly. Critics say these rules force private companies to help the government spy on people. Experts believe these rules go against important privacy principles like only collecting necessary data and using it for specific purposes. The requirement to store data even without a security problem could lead to misuse and harm user privacy. As a result, India's cybersecurity system focuses more on government control and following orders than on protecting individuals' privacy and ensuring fair procedures.

Constitutional Challenges and Judicial Responses

Legality of Surveillance Powers

Using the Puttaswamy framework shows big problems in how India's surveillance system works. The first part of this framework, called legality, says that any rules that limit basic rights must come from a clear, easy-to-understand, and specific law made by Parliament. But most of the powers that allow surveillance in India come from orders made by the executive branch or lower-level laws, like the IT Rules, not from detailed laws passed by Parliament. This breaks the legality rule and makes it easier for the executive to act without proper checks, putting citizens at risk of unfair treatment

Necessity and Proportionality

The second and third points—necessity and proportionality—mean that government actions must be carefully designed and use the least harmful method possible. Section 69 of the IT Act gives wide powers to intercept communications without needing specific reasons for each case or time limits. This lack of personal checks or court approval results in broad and unfair invasions of privacy. Without clear rules or requirements to report, these powers might be used for political reasons instead of real security needs.

Absence of Procedural Safeguards

A big problem in the constitution is that there is no independent check in place. The committees set up under the 2009 rules are made up only of government officials, which means they are regulating themselves instead of being truly accountable. People being watched aren't told about it by law, there is no court review after the fact, and there is no separate check on the activities of monitoring. This lack of proper oversight hurts fairness in the process and allows secret surveillance without any way to appeal or know what is happening.

Judicial Deference to National Security

Even though courts have sometimes stepped in, their actions have not been consistent. In the case of People's Union for Civil Liberties (PUCL) v. Union of India (1997)[9], the Hon'ble Supreme Court saw telephone tapping as a major violation of privacy and told the government to create proper rules to protect people's rights.

[8] *The Information Technology Act, 2000*

[9] *People's Union for Civil Liberties (PUCL) v. Union of India (1997) 1 SCC 301*

But later, these rules have not been followed properly. In recent years, courts have become more willing to accept the government's claims about national security, often without checking if the surveillance is justified. This pattern makes the Puttaswamy decision less effective and weakens the legal protection of privacy in the constitution.

Comparative and Reform Perspectives

Lessons from the European Union

The European Union sets an example with strong checks and balances on surveillance. Through rules like the General Data Protection Regulation (GDPR) and the NIS2 Directive[10], any action that involves personal data or affects digital privacy must be justified as necessary for a democratic society. Any surveillance activities must go through court checks and be watched over by independent groups that protect privacy. The GDPR also requires that data be used only for specific purposes, kept as simple as needed, and be clear to people. This makes sure that when the government accesses data, it's done only when really needed and in a responsible way.

The United Kingdom's "Double-Lock" Model

The United Kingdom's Investigatory Powers Act of 2016, often called the "Snooper's Charter," has a "double-lock" system for approving surveillance. This means that to get a warrant for spying, it needs both approval from the government and a judge-like person called a judicial commissioner. This two-step check makes sure that any spying is fair, necessary, and checked by someone independent. The UK also requires regular reports to Parliament and has an independent group, the Investigatory Powers Commissioner's Office, to oversee everything. This helps keep things open and honest without stopping real security work.

Reform Proposals for India

India's cybersecurity and surveillance system could improve by using similar accountability measures. Instead of having many different rules made by the government, there should be one clear law that covers all surveillance. This law should explain exactly what kind of surveillance is allowed, how long it can last, and why it is needed. Before any monitoring happens, there should be a court or a body that acts like a court that approves it. All surveillance efforts should be reported to the parliament, checked by an independent reviewer, and looked at again after the fact. The law should also include important rules like only collecting the minimum amount of data needed, using the data for specific reasons, and keeping it for a limited time. These rules help make sure that surveillance is fair and not too broad. Also, people should have the right to challenge and get help if they feel their privacy was violated through improper surveillance.

III. Conclusion

India stands at a constitutional crossroads between safeguarding national security and upholding the right to privacy. The Puttaswamy judgment proved privacy as a fundamental right, but its enforcement has been undermined by an expansive and opaque surveillance regime. The absence of legislative safeguards, judicial oversight, and transparency mechanisms has created a structural imbalance in favor of executive discretion. Learning from global best practices—particularly the European Union and the United Kingdom—India must move toward a legal framework that reconciles security imperatives with constitutional freedoms. Robust oversight, legal clarity, and independent accountability are not obstacles to national security—they are its democratic foundation.

IV. Suggestions

- Enact a dedicated Surveillance Reform Act outlining lawful interception procedures and accountability mechanisms.
- Establish an Independent Oversight Authority to review and authorize surveillance requests.
- Integrate judicial authorization for interception and data access.
- Ensure parliamentary reporting and transparency for cybersecurity measures.
- Harmonise the Data Protection Act and Cybersecurity Framework to create a unified, rights-based digital governance model.

[10] *Directive (EU) 2022/2555 (NIS2 Directive) on measures for a High Common Level of Cybersecurity.*