BALANCING NATIONAL SECURITY & INDIVIDUAL PRIVACY: A CONSTITUTIONAL APPRAISAL UNDER ARTICLE 21

Yashika Ashok Porwal, LL.M., School of Law, Christ (Deemed to be University), Bengaluru, India

ABSTRACT

The paper is a critical analysis of the constitutional elements of tension between national security and the fundamental right to privacy in India, especially under Article 21 of the Indian Constitution. The study uses a doctrinal and comparative legal approach to examine the changing jurisprudence (after K.S. Puttaswamy 2017) and the surveillance framework of India, such as the Indian Telegraph Act, Information Technology Act, Aadhaar Act, and the Digital Personal Data Protection Act of 2023. The paper determines the major gaps, including but not limited to the disjointed legal system, too much discretion in the hands of the executive, and lack of judicial control that erode privacy guarantees despite the constitutional requirements. Experiences in the United States and the United Kingdom demonstrate a positive result of extensive statutory systems and autonomous control tools. The results underscore the necessity of India coming up with a single, transparent, and constitutionally consonant surveillance law that would balance the need to maintain national security and the privacy rights of the citizens. The study is part of the wider debate on democratic accountability and the protection of human rights in digital space.

Keywords: National Security, Right to Privacy, Surveillance, Article 21

1. Introduction

The fast infiltration of technology in the current digital era has increased the surveillance ability of the state, which creates important constitutional issues that deal with the conflict of national security to the privacy rights of an individual.[1] Governments all over the world are constantly utilizing advanced surveillance techniques based on the threat of terrorism and cybercrime as it is necessary in national sovereignty and security.[2] The situation in India is particularly unique as the country is the largest democracy in the world, and its peculiarities are the hybridization of the legislation, including the laws of the colonial period as well as the modern ones and the high level of technological surveillance.[3] This legal heterogeneous environment consists of the most critical legislation, such as the Indian Telegraph Act, 1885; the Information Technology Act, 2000; the Aadhaar Act, 2016; and the Digital Personal Data Protection Act, 2023.[4] It also has many surveillance systems such as Central Monitoring System (CMS), the National Intelligence Grid (NATGRID), and Network Traffic Analysis (NETRA).[5] In spite of this technological complexity, this hybrid legal system faces colossal gaps of clear, overall legal safeguards, a dearth of judicial accountability, and openness leading to greater corporate dangers of state power misuse and intrusion on privacy.[6]

This research is significant because the Supreme Court made a historical decision in K.S. Puttaswamy v. Privacy was constitutionally established as a basic right (Article 21), and union of India (2017) recognized that right.[7] The decision requires that any state action imposing anti-privacy should meet the requirements of legality, necessity, and proportionality, which redefines the constitutional environment of surveillance control in India.[8] Nevertheless, the lack of a single surveillance law and the existence of pieces of recycled provisions have left a vacuum in the regulatory framework, allowing unhindered executive discretion and little independent control. [9]The Pegasus spyware scandal is an example of the harms of such legal gray area and indicates the misuse of surveillance technology to infringe upon privacy, de-

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶ 297 (India).
[2] United Nations Office on Drugs & Crime, The Use of the Internet for Terrorist Purposes 3–6 (2012).
[3] Shubhankar Dam, Privacy and Surveillance in India, 8 NUJS L. Rev. 1, 4–6 (2015).
[4] Information Technology Act, No. 21 of 2000, §§ 69, 69A, 69B (India).
[5] Centre for Internet & Society, *India's Surveillance State* (2014).
[6] Usha Ramanathan, Aadhaar: From Welfare to Surveillance State, 50 Econ. & Pol. Wkly. 33, 36–38 (2015).
[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 3, 297 (India).
[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶ 325 (India).
[9] Parliamentary Research Service India, The Right to Privacy and Surveillance in India (2017).

escalate the freedom of expression, and suppress democracy.[10]

One of the biggest gaps in the research is the lack of integrative study of the surveillance legislation in India both nationally and internationally, especially in the wake of development of digital surveillance and modern jurisprudence of privacy.[11] Although the Indian legal literature has covered privacy rights and judicial declarations, there is still a lack of the overall consideration of statutory provisions, control processes and global best practices that can inform trying the change.[12] The comparative views of other democracies like the United States and the United Kingdom on the benefits on overall laws of surveillance along with the presence of independent surveillance courts and regulatory agencies which will ensure that the surveillance is proportional and necessary will offer useful guidelines to India.[13]

This paper, then, reviews the legal and constitutional aspects of surveillance and privacy that have been changing in India, evaluating the sufficiency of the laws and the feasibility of the surveillance systems in consideration of the constitutional provisions.[14] It contextualizes this question in the wider context of the global discussion of privacy and security in the world and puts an analytical approach based on comparison to outline the shortcomings and lead to changes.[15] The study will shed light on the strains involved in the balancing of state security purposes with individual privacy rights and propose an effective, clear, and constitutionally acceptable system of surveillance.[16]

The particular aims of the study are to critically analyse the judicially accepted right to privacy in the Article 21; assess the legality, necessity, and proportionality of the major Indian surveillance laws and systems including the Indian Telegraph Act, IT Act, Aadhaar Act, CMS and NATGRID and NETRA; interpret any weaknesses in the transparency, monitoring and accountability; compare Indian statutory and institutional surveillance mechanisms to those of the US and the UK and suggest a balanced legal framework that can safeguard the interests of

[10] Manohar Lal Sharma v. Union of India, (2021) 10 S.C.C. 1, ¶¶ 27–30 (India).
[11] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 3–5 (2020).
[12] Vidushi Marda, India's Surveillance Framework: A Legal and Constitutional Analysis, Centre for Internet & Society(2018).
[13] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c; Investigatory Powers Act 2016, c. 25, §§ 227–236 (U.K.).
[14] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 180–181 (India).
[15] OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).
[16] David Cole & Federico Fabbrini, Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders, 14 Int'l J. Const. L. 220, 224–27 (2016).

democracy and must meet the needs of national security.[17] This study brings value to the crucial debate on the protection of individual rights in the era of broad based state surveillance by connecting the constitutional promises with the reality of governance.[18]

3. India's Fragmented Surveillance System

The national security interests and privacy rights of India are complicated and fragmented, and the national security laws are held by colonial Acts and modern laws, and not just one specific law on surveillance.[19] This legal regime has a large operation risk of breaching constitutional norms and fulfilling security aspects, which is markedly different as compared to more prescriptive policies, which comprises the margins of the law in other jurisdiction, including the United States and the United Kingdom.[20]

3.1 The Indian Telegraph Act, 1885: Colonial Foundations in the Digital Age

Despite Indian Telegraph Act of 1885, which has colonial origins and was written earlier than the digital era, retains its role in establishing the foundation of authority to surveil in India.[21] Section 5(2) of the Act gives the central and state governments the authority to intercept communications during an emergency or in order to promote public safety where it is related to the sovereignty, integrity, national or public safety.[22] People's Union for Civil Liberties (PUCL) v. The Supreme Court, in Union of India (1997), also put procedural conditions on interception, such as an approval of a competent authority, and review by specified committees, but not judicial review, and placed the executive branch and procedural requirements as the ultimate accountability measure.[23] The use of this colonial law raises the basic constitutional issues on privacy rights.[24] Specifically, the Act is too broad in its definitions of interception of communications in case of a public emergency or a public safety, and thus lacks the specificity required to be constitutional under the legality component of Puttaswamy, and the process

[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[18] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 7–9 (2020).
[19] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301, ¶¶ 18–20 (India).
[20] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c; Investigatory Powers Act 2016, c. 25 (U.K.).
[21] Indian Telegraph Act, No. 13 of 1885 (India).
[22] Indian Telegraph Act, No. 13 of 1885, § 5(2) (India).
[23] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301, ¶¶ 35–38 (India).
[24] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶ 297.

provisions fail to sufficiently capture the technological surveillance norms of the digital era.[25]

3.2 Information Technology Act, 2000: Surveillance of the Digital World in the Absence of proper protection.

The major digital surveillance regime in India is stipulated by the Information Technology Act to the extent that, Sections 69, 69A, and 69B provide the government with a wide power to intercept, monitor, decrypt, or block access to digital communications and computer resources. [26] They allow interactions to take place based on defined justifications with regards to the sovereignty and territorial integrity of India, the security of states, cordial ties with exogenous nations, civility and averting any cognizable crimes.[27] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, have given certain procedural requirements but critics argue that the procedures were too dependent on the executive discretion instead of meaningful judicial review.[28] The surveillance measures in the Information Technology Act give much too broad an area in regards to the scope, and it does not have enough narrow safeguards to check the abuse of power by the government and is beneficial in the area of ensuring privacy.[29] The procedural apparatus creates a wholesome executive-effective system of authority to conduct activity control without judicial guidance which can be inconsistent with the constitutional requirements on independent assessment when denying the basic rights.[30] There is also a 180-day period of authorization of surveillance activity (reviewable) in the Rules that permits a massive amount of time and activity to invade the privacy in a completely ex parte manner with no accountability.[31]

3.3 Aadhaar Act, 2016: A Surveillance Capable Welfare Architecture.

The Aadhaar Act, 2016, which was initially founded as a welfare-delivery law, is now increasingly pertinent to the surveillance architecture in India by how it is designed and the

[25] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[26] Information Technology Act, No. 21 of 2000, §§ 69, 69A, 69B (India).
[27] Information Technology Act, No. 21 of 2000, § 69(1) (India).
[28] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 3; Vidushi Marda, *India's Surveillance Framework: A Legal and Constitutional Analysis*, Centre for Internet & Society (2018).
[29] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 10–12 (2020).
[30] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[31] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 9.

data necessities it entails as well as the volume of biometric information it makes central.[32] Although the idea of the Act is as a means to help make the delivery of the effective public service a sure thing, the creation of a unified centralized database with a biometric identification (iris scans, fingerprints) surely brings the fear of the functionality creep, discrimination, and a possibility to easily track the citizen in various areas.[33]

The Act gives Aadhaar a mandatory impact on access to subsidies and benefits in Section 7, and addresses data protection in Sections 28-33; but their protection has been generally deemed to be inadequate.[34] The lack of effective purpose restriction, effective independent control, or direct restrictions on connecting Aadhaar with other databases presents a weakness that will result in a misuse of surveillance.[35]

In the case of K.S. Puttaswamy (Aadhaar) (2018), the Supreme Court approved the Act, but expressly noted the dangers of profiling, asking the government to decouple Aadhaar with the private services and limiting its compulsory utilisation.[36] However, the practical structure of the CIDR (Central Identities Data Repository) and the application of Aadhaar-based eKYC and large-scale adoption of the same by the private sector before the ruling, made Aadhaar a factual digital identity infrastructure.[37]

Constitutionally, the Aadhaar ecosystem has difficulties in complying with the requirement of necessity and proportionality that is in Puttaswamy since:[38]

- Authentication trails generate metadata which can give an insight into behavioural patterns of the users.[39]

- No separate data protection authority exists that has surveillance oversight roles; and[40]

[32] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, *supra*note 9.
[33] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1, ¶¶ 447–449 (India).
[34] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, *supra*note 32, §§ 7, 28–33.
[35] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, *supra* note 33, ¶¶ 447–452.
[36] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1, ¶¶ 447–448, 451 (India).
[37] Usha Ramanathan, The Architecture of Aadhaar: Surveillance, Profiling and Function Creep, 54 Econ. & Pol. Wkly. 38 (2019).
[38] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[39] Usha Ramanathan, Aadhaar: From Welfare to Surveillance State, 50 **Econ. & Pol. Wkly.** 33, 36–37 (2015).
[40] Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians 112–14 (2018).

- The Act permits a wide access of authentication logs by the government when the act is used under national security (Section 33(2)) and there are no substantial checks.[41]

Therefore, although Aadhaar is not a traditional surveillance law, its design allows the state to have an unprecedented level of population-wide surveillance and profiling, which poses serious constitutional issues under articles 14, 19, and 21.[42]

3.4 Central Monitoring System (CMS): Real-Time Telecommunication Surveillance: Institutionalised.

The Central Monitoring System (CMS), which was introduced by the Department of Telecommunications is one of the most advanced domestic surveillance systems in India.[43] It aims at direct, centralized, and real-time access to all telecom communications, voice calls, text messages, social media usage, and metadata and not necessitate individual interception request to pass through Telecom Service Providers.[44]

CMS is an executive-architecture, lacking a full statutory basis; the operation of CMS occurs under the jurisdiction of Telegraph Act and the IT Act.[45] The lack of a discrete legal system causes CMS to carry all the disadvantages of these piecemeal colonial and digital-era laws, most notably, the lack of judicial review, ambiguity on the limits of interception, and executive power concentration.[46]

Unlike the traditional method of interception that requires telecom companies to arbitrate, CMS means that the government does not need commercial brokers, whatsoever, leading to a silent, centralized, and opaque system.[47] Critics believe that this minimizes friction which has traditionally acted as a control on wanton spying and undermines openness.[48]

CMS constitutionally does not coexist with the procedural protections necessary to

[41] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, § 33(2) (India).
[42] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, *supra* note 33, ¶¶ 447–452.
[43] Department of Telecommunications, Govt. of India, *Central Monitoring System (CMS).*
[44] Centre for Internet & Society, India's Central Monitoring System: Architecture, Risks and Legal Gaps (2015).
[45] Ibid.
[46] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 180–181, 325–326.
[47] Centre for Internet & Society, India's Central Monitoring System: Architecture, Risks and Legal Gaps (2015).
[48] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 13–15 (2020).

Puttaswamy, in that:

1. It facilitates mass, dragnet-like access, without case-sensitive authorisation;[49]

2. It does not have an independent checking body or a parliamentary check.[50]

3. There is no post-facto compensation or even notice (after investigations have been completed).[51]

CMS therefore constitutes a change in focus whereby interception is replaced by infrastructure level surveillance, increasing the chances of a disproportionate violation of rights.[52]

3.5 NATGRID: Interconnected Intelligent and Predictive Surveillance Data Banks.

The National Intelligence Grid (NATGRID) is created as a combined data-fusion system that brings together more than twenty-four databases (travel, bank, PAN, immigration, telecommunications, and others) in order to enable quick access to information by the law enforcement and intelligence services.[53]

NATGRID does not have a particular statute but administrative orders.[54] Profiling and pattern analysis is made possible by the ability to query multiple datasets in real-time because of its architecture.[55] The system is also available to various intelligence agencies, such as the IB, RAW, NIA and DRI to name a few, thus its surveillance capabilities are much wider as compared to the traditional investigative instruments.[56]

The absence of a statutory foundation of the system creates severe rule-of-law issues:

1. There are no legislative limitations of purpose or data-minimisation.[57]

[49] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[50] Centre for Internet & Society, India's Central Monitoring System: Architecture, Risks and Legal Gaps (2015).
[51] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301, ¶¶ 35–38 (India).
[52] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 14–16 (2020).
[53] Ministry of Home Affairs, Govt. of India, National Intelligence Grid (NATGRID).
[54] Centre for Internet & Society, India's Surveillance State: NATGRID and the Legal Vacuum (2017).
[55] Ministry of Home Affairs, Govt. of India, National Intelligence Grid (NATGRID).
[56] Parliamentary Standing Committee on Home Affairs, Demands for Grants (2019–20): Ministry of Home Affairs, ¶¶ 42–44.
[57] Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians 112–14 (2018).

2. The queries raised, their motive and precautions are not judicially or otherwise monitored.[58]

3. The architecture is oblique and the citizens are not made aware whether or not their information is being accessed or profiled.[59]

NATGRID is currently incapable of meeting the legality, necessity, and proportionality criteria in the context of expert supervision by Puttaswamy, as predictive surveillance and data-fusion surveillances can effortlessly surpass their required law-enforcement demands.[60] It also runs the risk of establishing a surveillance atmosphere in which behavioural analytics and profiling take place with no constitutional or statutory constraints.[61]

3.6 NETRA: Surveillance by Automated Interception, AI-Driven Surveillance and the Pivot to Invasive Surveillance of the Mass.

One of the AI-based, automated, and proactive surveillance tools developed by DRDO is NETRA (Network Traffic Analysis), which reflects the transition of India to this kind of surveillance.[62] NETRA is intended to scan internet traffic containing keywords that may be used to threaten national security and monitors social media, email, chat applications, and online communications in real time.[63]

Its use is similar to the early world deep-packet-inspection and keyword-monitoring systems. Nevertheless, the system does not have a publicly known statutory foundation but instead it is founded on internal government authorisations.[64]

The constitutional problems are heightened since:

1. Watching using a keyword will inevitably lead to broad coverage of data.[65]

[58] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 180–181, 325–326.
[59] Centre for Internet & Society, India's Surveillance State: NATGRID and the Legal Vacuum (2017).
[60] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[61] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 15–17 (2020).
[62] Defence Research & Development Organisation (DRDO), Govt. of India, *NETRA—Network Traffic Analysis System: Project Overview*.
[63] Anja Kovacs & Vidushi Marda, Surveillance in India: NETRA, CMS and the Legal Vacuum, Centre for Internet & Society (2017).
[64] Ibid.
[65] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.

2. The filtering based on AI is untransparent and can disfavor minorities, activists, or even people involved in political opposedness.[66]

3. there is no meaningful way to challenge or even review the outputs or errors of the system by its users;[67]

4. No published oversight mechanism, audit trail or accountability structure.[68]

On the rights perspective, NETRA involves:

1. Article 21 (privacy and autonomy),[69]

2. Article 19(1)(a) (Speech and expression).[70]

3. Article 14 (non-arbitrariness).[71]

Surveillance is an automatized process that can put the online speech on chilling and establish an atmosphere of omnipresent monitoring that does not correspond to democratic liberties.[72] Neither of the two has a legislative basis, which puts NETRA beyond the legality requirement of Puttaswamy and therefore makes it constitutionally questionable.[73]

4. The Contemporary Surveillance Systems: Legal Vacuum.

Nowadays, surveillance opportunities are based on advanced systems that act in accordance with the general executive authority with no legislative support.[74] Central Monitoring System (CMS) allows real-time interception of telecommunications without the participation of the telecommunications service provider, and the National Intelligence Grid (NATGRID) allows coordinating multiple government databases on the national level into a unitary project of

[66] U.N. Special Rapporteur on the Promotion & Protection of the Right to Freedom of Opinion & Expression, *Report on Surveillance and Human Rights*, ¶¶ 53–56, U.N. Doc. A/HRC/41/35 (2019).
[67] Manohar Lal Sharma v. Union of India, (2021) 10 S.C.C. 1, ¶¶ 27–30 (India).
[68] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 16–18 (2020).
[69] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 297–298.
[70] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1, ¶¶ 90–94 (India).
[71] E.P. Royappa v. State of Tamil Nadu, (1974) 4 S.C.C. 3, ¶¶ 85–87 (India).
[72] U.N. Special Rapporteur on the Promotion & Protection of the Right to Freedom of Opinion & Expression, *Report on Surveillance and Human Rights*, ¶¶ 20–24, U.N. Doc. A/HRC/41/35 (2019).
[73] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[74] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 8–10 (2020).

intelligence analysis.[75] Defence Research and Development Organisation has come up with Network Traffic Analysis (NETRA) which tracks on the keywords and patterns carried in unencrypted traffic in the internet.[76] All these three systems are an indication of a new degree of surveillance potential.[77]

All this, begs critical questions of legal authority, transparency and constitutional compliance since they usually work in absolute secrecy with general executive articulations the only formal enabling document.[78] The absence of official authority to authorise such moves is at worst a legal vacuum situation, as scholars and critics of recent surveillance trends put it.[79] With this infrastructure of mass surveillance, it is possible to collect data in bulk quantities beyond the proportionate measure of just targeting surveillance, therefore, surpassing the measure considered and outlined as non-invasive reaction in R. v. Puttaswamy[80].

4.1 Constitutional Evolution: From Denial to Fundamental Right

1. **Historical Judicial Development**

The concept of privacy as a fundamental right in India has developed over a long history of judicial incremental development.[81] In M.P. Sharma Case and in Kharak Singh Case(1954), the first judicial office categorically ruled out privacy as a fundamental right but in the same case.[82] The issue of privacy is prescient in the state of Uttar Pradesh (1963) which stated that it is possible to have privacy under Article 21.[83] This was climaxed in the landmark case of K.S. Puttaswamy.[84] In a case that had a 9-judge bench, which was unanimous, Union of India (2017) established that privacy is a fundamental right guaranteed in Articles 14, 19, and 21 of the Constitution.[85]

---

[75] Centre for Internet & Society, India's Central Monitoring System: Architecture, Risks and Legal Gaps (2015).
[76] Ministry of Home Affairs, Govt. of India, National Intelligence Grid (NATGRID).
[77] Anja Kovacs & Vidushi Marda, Surveillance in India: NETRA, CMS and the Legal Vacuum, Centre for Internet & Society (2017).
[78] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 8–10 (2020).
[79] Anja Kovacs & Vidushi Marda, Surveillance in India: A Legal and Constitutional Vacuum, Centre for Internet & Society (2017).
[80] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[81] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 19–22 (India).
[82] M.P. Sharma v. Satish Chandra, A.I.R. 1954 S.C. 300; Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295.
[83] Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295, ¶¶ 18–20.
[84] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 81.
[85] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 81, ¶¶ 297–298.

1. **An Approach to Surveillance Regulation: The Three-Pronged Constitutional Test.**

1. Legality: Rights against violating personal privacy should be the express, definite legal authorization, as opposed to merely the exercise of a statutory discretion.[86] This need presents a direct problem to existing Indian surveillance practices that depend on imprecise statutory phrasing on the outmoded law that has no explicit requirements of adherence to the Constitution.[87]

2. Legitimate Aim/Necessity: The restriction of the privacy should be grounded in a bona fide and provable purpose by the state but the mere or ambiguous claim of national security or public order is not a sufficient reason unless substantiated by particular articulations of the necessity of the state.[88] This has occurred on numerous occasions even though it has been argued that privacy is limited on the basis of necessity, but without any particular determination or claim of danger, peril, or intimidation.[89]

3. Proportionality: The surveillance method must be appropriate to the legitimate purpose being pursued, and the method must utilize the minimum intrusion method possible, and must not extend beyond what is needed to fulfill the mentioned purpose.[90] Systems like the CMS and NATGRID allow the surveillance to greater levels than legitimate security objectives, and are necessarily disproportionately intrusive.[91]

5. Post-Puttaswamy Jurisprudential Challenges

The decision in Puttaswamy had ominous effects on future cases, e.g. Manohar Lal Sharma v. In the case Union of India (2021), in which the Supreme Court considered the surveillance matter of the spyware Pegasus, it once again concluded that any intervention of a state into the life of the population should also be legislatively glorified and should also be reviewed by the court. [92]The events of Pegasus indicate that surveillance authority can be misused and directed against the journalists, political opposition, activists, and civil society as state adversaries.[93]

[86] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 325–326 (India).
[87] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 9–11 (2020).
[88] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 325–326 (India).
[89] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637, ¶¶ 68–71 (India).
[90] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 325–326 (India).
[91] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 15–17 (2020).
[92] Manohar Lal Sharma v. Union of India, (2021) 10 S.C.C. 1, ¶¶ 27–30 (India).
[93] Manohar Lal Sharma v. Union of India, *supra* note 92, ¶¶ 41–44.

The problems of Pegasus show that surveillance authority may destroy the democratic operation and the constitutional rights.[94]

5.1 Legislative Attempts at Data Protection: The DPDP Act's Progress and Pitfalls

The Digital Personal Data Protection Act, 2023, has become the most recent attempt to govern the operations of personal data processing in India to create a middle ground between the privacy rights of any individual and the issue of national security.[95] The Act creates the accountability, transparency and protection of personal data as well as mandating the direct consent of the individual in relation to their data to be processed.[96] Section 7(c) is very clear that surveillance procedures must be reasonable and justified in the name of national security and national safety.[97] However, DPDP Act has faced severe criticism due to many exemptions that might erode the privacy of people.[98] Section 17(2)(a) offers an exception to government bodies to the provisions of the Act in situations where it handles the personal data of a national security, public order, sovereignty and integrity of India, or prevention of a cognizable offense.[99] Opponents argue that the exemptions are too wide-ranging and imprecise to enable narrow surveillance with limited judicial controls or other checks and balances, which might lead to the Swiss cheese strategy.[100]

5.2 Weaknesses in Institution and gaps in enforcing these rules.

The establishment of the Data Protection Board of India (DPBI) under the Act has been lamented as having a very limited adjudicative role and not having any significant regulatory powers to question government surveillance schemes or change the privacy laws to suit technological developments.[101] The absence of any significant consent-based restrictions on government surveillance practices and the lack of the independent judicial check and balance on the exempted activities forms a legal framework that facilitates constitutional breaking as

[94] Amnesty Int'l, Forensic Methodology Report: How to Catch NSO Group's Pegasus (2021).
[95] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[96] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–6 (India).
[97] Digital Personal Data Protection Act, No. 22 of 2023, § 7(c) (India).
[98] Vidushi Marda & Meghna Bal, India's Data Protection Bill: Between Surveillance and Privacy, Centre for Internet & Society (2023).
[99] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(a) (India).
[100] Shubhankar Dam, Exemptions, Executive Power and the DPDP Act, 58 Econ. & Pol. Wkly. 12, 14–16 (2023).
[101] Apar Gupta & Abhinav Sekhri, India's DPDP Act: Weak Regulator, Strong Executive, Internet Freedom Foundation(2023).

opposed to stopping it.[102]

6. Comparison International Frameworks: US and UK Lessons.

6.1 United States: Organized Supervision and Continuous Problems.

The United States has a national security surveillance system of multi-layers and some of the key legislative frameworks are well structured as compared to India.[103] The Foreign Intelligence Surveillance Act (FISA) of 1978 created the Foreign Intelligence Surveillance Court (FISC) which serves as a specialized judicial provider with regard to monitoring the actions of foreign intelligence targets, a form of judicial position that is not available in the executive-only scheme in India.[104]

Although the Fourth Amendment does not use the word privacy, the Fourth Amendment forbids unreasonable search and seizure, which has been applied judicially to give considerable digital privacy protection, particularly since Carpenter v. United States (2018) in which historical cell phone location data could only be accessed with a warrant.[105] It acts as a better foundation protection to privacy compared to Article 21 of the Indian Constitution which had to be interpreted by the court of law in order to recognize the right to privacy.[106]

- **Reforming Evolution: The PATRIOT Act to the FREEDOM Act.**

The USA PATRIOT Act original broad surveillance authorities were checked by the USA FREEDOM Act of 2015 that not only terminated the collection of metadata in bulk but also demanded the specific judicial authorization to access telecommunications information.[107] This history of legislation shows that in democratic states, surveillance can be checked against excessive surveillance by law, unlike in India where unlimited surveillance can be made more permanent.[108]

---

[102] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 7, ¶¶ 325–326.
[103] David Cole & Federico Fabbrini, Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders, 14 Int'l J. Const. L. 220, 224–26 (2016).
[104] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1813 (establishing the Foreign Intelligence Surveillance Court).
[105] Carpenter v. United States, 138 S. Ct. 2206, 2217–19 (2018).
[106] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 297–298 (India).
[107] USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 101–103, 129 Stat. 268 (codified as amended in scattered sections of 50 U.S.C.).
[108] David Cole, After Snowden: The Legal and Political Consequences of Surveillance Reform, 34 Yale L. & Pol'y Rev. 1, 6–9 (2015).

Federal courts have affirmed the restrictions on certain types of surveillance and attacked federal surveillance when there is adequate evidence.[109] In ACLU case, the Court ruled that the bulk metadata collected by the NSA was unlawful, as it violated the privacy right of people and was done without any statutory authorization on how to do so (Clapper, 2015). The courts are eager to examine the surveillance powers of the government in a way that Indian courts never had the tradition of doing.[110]

6. 2 United Kingdom: Complete Framework and Independent Supervision.

- **Investigatory Powers Act 2016: Safeguarded Structured Surveillance.**

One of the broadest surveillance regimes in the democratic world, the Investigatory Powers Act (IPA) 2016 in the United Kingdom has brought together numerous previous legislations alongside a broad-ranging supervision.[111] Under the Act, the surveillance warrants can be approved both by ministerial authorization and the judicial decision, which means that this method of surveillance is more closely regulated than the Indian system of surveillance that was based on the executive.[112] In the United Kingdom, the European Convention on human rights which has been incorporated in the Human Rights Act 1998 under Article 8 offers privacy rights.[113] This Article puts binding duties that proportionality and necessity must be considered before engaging in surveillance. Nonetheless, these safeguards can be trusted upon after a legally commissioned surveillance.[114] The Office of the Investigatory Powers Commissioner (IPCO) is an autonomous body, which offers supervision and thus routine checks, audits and scrutiny of surveillance processes, which is delivered by reports of annual public scrutiny by the IPCO.[115]

- **Judicial Review and International Human Rights Compliance.**

The UK courts have been able to restrict the surveillance, where it is beyond the legal scope.[116]

---

[109] ACLU v. Clapper, 785 F.3d 787, 818–21 (2d Cir. 2015).
[110] Abhinav Chandrachud, Judicial Review of Surveillance in India, 7 Indian J. Const. L. 145, 156–59 (2019).
[111] Investigatory Powers Act 2016, c. 25 (U.K.).
[112] Investigatory Powers Act 2016, c. 25, §§ 19–23 (U.K.).
[113] Human Rights Act 1998, c. 42, sch. 1, art. 8 (U.K.).
[114] Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14 & 24960/15, Eur. Ct. H.R. ¶¶ 323–325 (2021).
[115] Investigatory Powers Commissioner's Office, Annual Report of the Investigatory Powers Commissioner (U.K.).
[116] Privacy Int'l v. Investigatory Powers Tribunal, [2019] UKSC 22, ¶¶ 131–134 (U.K.).

In Privacy International case, the UK Supreme Court determined in Investigatory Powers Tribunal (2019) that decisions of the surveillance tribunal can be reviewed in the court and this move has contributed to the introduction of accountability to the intelligence agencies.[117] In the case of the Big Brother Watch the European Court of Human Rights determined that the UK bulk interception regime infringed upon the right to privacy and the right to freedom of expression in some aspects in Big Brother Watch v. United Kingdom (2021), and there are reforms that continue to work on the shortcomings of the UK approach.[118]

6.3 Comparative Analysis: Systemic Weaknesses in India.

Compared to the all-inclusive supervision systems of surveillance in the US (the FISA courts) and the UK (with double-lock authorization and independent oversight), regulation and surveillance in India are carried out virtually through executive discretion with minimal transparency.[119] The decentralization of law making authority as was founded on the colonial period legislation leaves loopholes in the law system that govern digital surveillance.[120] The absence of dedicated judges, oversight bodies, or material judicial scrutiny of surveillance is constitutionally unpredictable.[121]

- **Dominance by the Executive and Lack of Judicial Checks and Balances.**

The surveillance regime in India is typified by executive self-regulation meaning that any order to undertake the surveillance is approved and vetted by the committees within the same government system that did the surveillance.[122] This brings about fundamental clashes of interest and discourages objectivity.[123]

7. Conclusion

This paper shows that the surveillance framework of India is at complete variance with the constitutional standpoints which have been laid down in K.S. Puttaswamy v. Union of India

[117] Privacy Int'l v. Investigatory Powers Tribunal, *supra* note 116, ¶¶ 144–147.
[118] Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14 & 24960/15, Eur. Ct. H.R. ¶¶ 323–325 (2021).
[119] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1813; Investigatory Powers Act 2016, c. 25, §§ 19–23 (U.K.).
[120] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301, ¶¶ 18–20 (India).
[121] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 325–326 (India).
[122] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301, ¶¶ 35–38 (India).
[123] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 180–181, 325–326 (India).

(2017).[124] Although the Supreme Court of India reiterated privacy as the primary right in Article 21 and introduced the most rigorous three-part test of legality, necessity, and proportionality, the legal system remains disjointed in India and operates under the laws of the colonial era and the new laws lacking adequate protection.[125] Accordingly, the regulatory gap permits the free executive enterprise at the cost of judicial review and responsibility to democracy.[126]

The relative comparison to the United States and the United Kingdom indicates the conspicuous flaws of India in terms of surveillance governance.[127] There is no effective independent executive regulation of self-regulation in India, unlike such democracies which have their own systems of judicial review, such as FISA courts in the US and the use of a double-lock authorization in the UK.[128] Complex surveillance programs, including CMS, NATGRID and NETRA, make use of privilege of law; they promote mass surveillance and act contrary to the constitutional principles.[129] The Pegasus scandal is an example of how this legal immunity interferes with institutions of democracy and civil freedoms.[130] The existing system of surveillance in India fails the constitutional test established by Puttaswamy: it is not legal (legality), not reasonable on the basis of a vague necessity (necessity) and it is mass surveillance that is disproportionate (proportionality).[131] Even the Digital Personal Data Protection Act, 2023, continues such violations with the broad scope of the exceptions concerning the purpose of the government, establishing the chilling effect on democracy and freedom of speech.[132]

Massive reform is necessary to carry out surveillance in a way that is consistent to the constitutional standards.[133] This would include a single surveillance law that explicitly defines the limits of government application, the creation of an obligatory judicial control, the

[124] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 297–298 (India).
[125] Justice K.S. Puttaswamy (Retd.) v. Union of India, *supra* note 124, ¶¶ 325–326.
[126] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 18–20 (2020).
[127] David Cole & Federico Fabbrini, Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders, 14 Int'l J. Const. L. 220, 224–27 (2016).
[128] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1813; Investigatory Powers Act 2016, c. 25, §§ 19–23 (U.K.).
[129] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 14–18 (2020).
[130] Manohar Lal Sharma v. Union of India, (2021) 10 S.C.C. 1, ¶¶ 27–30 (India).
[131] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 325–326 (India).
[132] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(a) (India).
[133] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 325–326 (India).

introduction of independent enforcers with practical powers, and openness to create democratic accountability. It is this radical reform that can enable India to have in place a surveillance regime that in a real sense can balance national interests of security with the right to privacy as enshrined in the Constitution and that furthers the cause of democratic governance as opposed to compromising human dignity in the digital era.[134]

[134] Shubhankar Dam & Rahul Bajaj, Surveillance, Privacy and the Constitution of India, 4 Indian L. Rev. 1, 20–22 (2020).