

Metadata, mass surveillance and criminal investigations in India: A post-*Puttaswamy* analysis

Adv. Neha Goyal, Ms Ananya Yadav

Abstract - In India, as digital ecosystems grow, criminal investigations have been conducted differently than ever before where metadata can be used as an investigative tool. Through the utilization of call detail records and how people use the internet, law enforcement has the ability to not just track people's actions but connect individuals with one another as well as predict crimes prior to occurring without actually needing to examine the content of the data. But due to the *KS Puttaswamy v. Union of India* ruling on the right to privacy being a fundamental right, this has allowed more scrutinized analysis when using metadata in metadata collection processes for criminal investigations. With the courts ruling the legality of metadata, they changed from determining the legality of the laws governing metadata collection to determining the constitutionality of these laws. The conflict at issue is very clearly defined: the courts have determined that there are protections under the Constitution that apply to people who collect metadata while also determining that metadata can be less intrusive than content. The use of metadata for aggregated collection creates intimate personal profiles which call into question the distinction of content or non-content when surveilling individuals. The laws governing the collection of personal data in India, namely Telegraph Act and IT Act, do not address issues arising from large-scale metadata collection. In light of these changes, this research paper will provide an evaluation of the opinion of the judiciary about surveillance based on metadata for criminal cases in India after the *Puttaswamy* case. It will discuss if there are adequate protections in place and the evolution of judicial reasoning as a mechanism for balancing state authorities. It will also suggest a reformulation of the legal concepts which give effect to both efficiency and

constitutional protections for the individual's right to privacy.

Keywords: Right to privacy, Metadata, IT Act, Telegraph Act, Indian Constitution, *KS Puttaswamy v. Union of India*, criminal investigations.

I. INTRODUCTION

In the digital age, criminal investigations do not start at the crime scene. They start with the digital trails. A phone call made at midnight, a location ping near a crime location, a series of IP logins, or communication between individuals can now be a crucial part of an investigation. This information, termed 'metadata', is perhaps one of the most potent tools available for criminal investigations.¹ Unlike the content of a phone call or a series of communications, metadata shows the pattern of human behavior: who called whom, when, where, and how often.² Metadata is increasingly being used for criminal investigations.

However, the increasing reliance on metadata creates a complex constitutional issue: is it permissible for the State to conduct surveillance on its citizens in the name of investigation without infringing on their right to privacy? This is a pertinent issue in India in light of a landmark judgment by the Supreme Court in Justice *K.S. Puttaswamy v. Union of India*,³ which recognized right to privacy as a fundamental right under Article 21 of the Indian Constitution. Thus, there is no room for a discussion on the right to privacy from a policy or convenience point of view. Rather, there is a constitutional mandate that clearly delineates its parameters.⁴ This shift will be particularly important

¹ Rudraksh Lakra, Abhijeet Shrivastava, "Confronting the Metadata Dilemma in India: A Turn to Context and Proportionality" 32 *International Journal of Law and Information Technology* eaac012 (2024).

² P. Arun, "A Mosaic of Dovetailing Laws: India's Communications Surveillance Regime" 7(3) *Indian Law Review* 363-386 (2023).

³ AIR 2017 SC 4161

⁴ Menaka Guruswamy, "Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors." 112

in relation to metadata based surveillance. Metadata has traditionally been considered less invasive or less revealing than content data, in as much as it does not directly indicate what a person has said or written. Yet in the digital world of today, such a distinction appears ever more tenuous. Metadata collected, stored and analyzed in large volumes can be very revealing of a person's intimate life, including their social affiliations, political views, religious practices, travel patterns, health concerns and behavioral proclivities.⁵ In a sense, metadata can be even more revealing than content data, especially in conjunction with algorithmic analysis and digital profiling. Metadata thus becomes a very important constitutional issue.

Despite the fact that the relevance of this issue is growing rapidly, Indian legal studies and Indian judicial discussions have not adequately addressed metadata as a distinct constitutional issue. In fact, a lot of the existing Indian discussion on surveillance has been broadly centered on phone tapping, internet shutdowns or general violations of privacy, such as spyware.⁶ Although these are certainly pertinent areas, they have, in a sense, failed to focus on the role of metadata in criminal investigations. There is a general lack of research on how Indian courts have dealt with metadata collection after the *Puttaswamy* judgment, whether Indian law adequately regulates such a practice, or how Indian law balances necessity with such a high degree of access to personal digital information.⁷

This is a pertinent issue because metadata is a grey area from a legal standpoint. It is commonly used by law enforcement agencies, though possibly not under as much public scrutiny or constitutional debate as communication interception.⁸ The current legal setup under the Indian Telegraph Act, 1885, Information

Technology Act, 2000, and surveillance regulations is largely a product of a different technological age, failing to capture the extent, detail and precision of modern metadata collection. There is a strong need to analyze whether India's current surveillance framework is compatible with the framework of privacy set out in *Puttaswamy*. In this context, the present paper attempts a critical analysis of the practice of using metadata and mass surveillance in criminal investigations in post-*Puttaswamy* India. The major submission of the present paper is that the practice of using metadata for the purpose of surveillance in criminal investigations needs to be recognized as a constitutionally sensitive practice with enhanced legal standards and greater accountability. Without such a shift in approach, the practice of using metadata for the purpose of surveillance would only result in the normalization of 'hidden forms of State surveillance' that negate the very concept of privacy upheld by the Supreme Court.

The study, therefore, aims to explore the legal position of metadata, constitutional restrictions on the use of metadata, the adequacy of India's surveillance regime, and the role of judiciary in striking an appropriate balance between security and the foundations of individual liberty.

II. UNDERSTANDING METADATA AND ITS ROLE IN CRIMINAL INVESTIGATIONS

While metadata has been referred to as "data about data," in a criminal investigation, it is much more than a mere by-product of technology. Metadata represents a systematic record of how, when, where, and between whom a communication or digital interaction

American Journal of International Law 144-150 (2018).

⁵ Arushi Gupta, "The Case Against the Constitutional Validity of Mass Surveillance Programmes" 3(3) *Indian Law Review* 225-253 (2019).

⁶ Samyukta Ramaswamy, "The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State" 20(2) *Indian Journal of Law and Technology*, Art. 4 (2024).

⁷ Jai Anant Dehadrai, Udipto Koushik Sarmah, "Surveillance, Criminal Investigations and Admissibility of Illegally Obtained Evidence: The Operationalisation of Privacy Post K.S. Puttaswamy" *SCC Online Times* (2022).

⁸ Vrinda Bhandari, Karan Lahiri, "The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-*Puttaswamy* World" 3(2) *University of Oxford Human Rights Hub Journal* 15-46 (2020).

occurred.⁹ Unlike content data, metadata does not indicate what a phone call, message, or email entails. What it does indicate are the surrounding factors, such as the length of a phone call, location coordinates, IP addresses, dates and times, device identifiers and patterns of communication.¹⁰ In the digital age, such pieces of information are not trivial. Indeed, they can collectively build a picture of an individual's activities, affiliations and behavioral proclivities with a high degree of accuracy.

From investigation perspective, metadata has proven to be indispensable to law enforcement agencies as it enables them to track relational and spatial patterns without necessarily intercepting the content of communications. It has been used to determine who was in contact with whom, whether a suspect was at a particular location, or whether particular individuals were in contact with each other as part of a criminal network.¹¹ From a research perspective, metadata can thus be considered behavioral evidence. It does not merely assist an investigation process. It actually informs the theory of a crime.¹²

In Indian criminal investigations, the most commonly used metadata is Call Detail Record (CDR), which contains information relating to the time of the call, the duration of the call, the source of the call, the destination of the call and the location of the tower from where the call was made.¹³ Internet metadata, including IP logs, internet logs, email headers and internet devices, is increasingly being utilised in internet crime investigations, fraud investigations,

organised crime investigations and internet conspiracy investigations. In a data-driven environment, metadata is often the first form of evidence by which law enforcement officials identify suspects.

The worth of metadata in a legal context is the possibility of its use as a lead or corroborating evidence. It could potentially connect the accused with the crime scene, create a connection between co-accused persons, or even contradict the account of an alibi. However, the increasing reliance on metadata also creates a larger constitutional problem: the relative lack of sensitivity of metadata compared with content data means that it is subject to a lesser level of legal and public scrutiny.¹³ This is no longer the case. The modern concept of metadata, particularly when used continuously and in bulk, has the potential to create a very detailed picture of a person's life. A pattern of late-night calls, regular visits to a medical facility, or the presence at a place of worship could reveal very intimate details of a person's identity or choices.¹⁴ Therefore, the relative invisibility of metadata is exactly the reason why it is a constitutional problem.

The difference between targeted surveillance and mass surveillance is particularly relevant at this point. In targeted surveillance, there is a collection of metadata based on a particular suspect or case. The collection is often for a particular purpose.¹⁵ In mass surveillance, the collection is much broader in scope. It is

⁹ Mattia Giangreco, 'Leveraging Metadata and Big Data for Criminal Investigations: Comparative Perspectives from Europe, USA and China' *IRIS* (2025).

¹⁰ Alana Maurushat, Lyria Bennett-Moses, David Vaile, 'Using "Big" Metadata for Criminal Intelligence: Understanding Limitations and Appropriate Safeguards' in *Proceedings of the 15th International Conference on Artificial Intelligence and Law (ACM) Western Sydney University* 196–200 (2015).

¹¹ Laura Neiva, Rafaela Granja and Helena Machado, 'Big Data Applied to Criminal Investigations: Expectations of Professionals of Police Cooperation in the European Union' 32(10) *Policing and Society* 1167–1179 (2022).

¹² Cheng Lei, 'Legal Control over Big Data Criminal Investigation' 40(3) *Social Sciences in China* 189–204 (2019). ¹³ R Aksietha, 'Surveillance in India and Its Privacy Challenges in the Digital Age: A Legal and Constitutional Analysis' 10(3) *International Journal for Research Trends and Innovation* (2025).

¹³ Vinay Kumar Singh & Veena Hada, 'Navigating the Digital Frontier with Privacy, Surveillance, and Data Protection in the Age of Datafication' 14(11) *Journal of Future Internet and Hyperconnectivity* 101–130 (2025).

¹⁴ Gagan C, 'Digital Panopticon: How Metadata Monitoring is Reshaping India's Democracy' 12(1) *Mainstream Weekly* 22–36 (2025).

¹⁵ Justin Clarke, 'Targeted Surveillance vs Mass Surveillance' *Australian Home Affairs* (2018).

sometimes not based on suspicion at all but is done to allow for future access or for intelligence analysis.¹⁶

The problem with mass surveillance is not only that it might be misused but that it might normalize the idea that citizens' digital lives are available to the State simply because technology allows for it. The concern becomes greater in the Indian context since the power of surveillance is usually exercised by the government. In other words, metadata is collected, stored or accessed through a mechanism that is not always traceable to the individual. In the absence of strong and comprehensive legislative protection, metadata can shift quickly from a tool for investigation to a means for prevention and profiling.¹⁷ In the field of criminal law, where freedom is a core issue, the question is one of constitutional examination.

The other important issue is the reliability of the evidence contained within metadata. Metadata is not necessarily free of interpretation difficulties, despite its reputation for objectivity and impartiality. Location information may indicate the general area of a particular device, but not necessarily the specific presence of a particular person or the specific activity of a particular person.¹⁸ Communication information may indicate contact, but not necessarily the purpose of the communication. Device information may be problematic because of shared devices, SIM card misuse, spoofing, and inaccuracies.¹⁹ Metadata is very valuable, but it cannot be relied upon by itself as a means of establishing guilt of a crime.²⁰

From a constitutional point of view, the real question is not whether the information is useful. It is clearly useful. The question is whether the use of the information is regulated, proportionate, and

accountable. Once the importance of privacy as a fundamental right is acknowledged, it is impossible to justify the unregulated treatment of metadata simply on the basis that it does not carry information about the content of speech or writing. In fact, the growth of digital policing makes the use of metadata one of the most significant areas through which the balance between investigative need and informational privacy is now defined. This is why, any meaningful discussion of surveillance in criminal law must go beyond the traditional approach to interception and direct monitoring, to recognize metadata as a key legal concept in its own right. It is no longer ancillary to criminal investigation; it is at its core.

The constitutional question, then, is not whether it may be relied on at all, but to what extent it may be relied on without threatening the privacy and liberty that the Constitution protects.²¹

III. LAWS GOVERNING METADATA SURVEILLANCE IN INDIA

The legal architecture of metadata surveillance in India is fragmented, executive-centric and technologically outdated. Even though India allows the State to intercept, monitor and access digital communications for legitimate reasons such as national security, maintenance of public order, and investigation of offenses, the legal architecture in India was not originally crafted for the level of technological advancement in metadata extraction. Although the Indian legal architecture allows the State to engage in surveillance activities, it does not offer much in terms

¹⁶ Chinmayi Arun, "Thin Safeguards and Mass Surveillance in India" 26(2) *NLSI Rev.* (2014).

¹⁷ Siddharth Johar, "Surveillance Backdoors and the Data Protection Regime in India" 12(2) *Indian Journal of Cyber Law & Policy* 45–70 (2025).

¹⁸ Baysah Guwor, Sridaran Rajagopal, S. Silvia Priscila, Dharmendrasinh D. Zala, "Reliability and Completeness of Metadata Extraction Tools in Image-Based Forensic Analysis" 2866 *AI & ML - Frontiers in Cross Disciplinary Applications & Case Studies* 1-20 (2026).

¹⁹ Aquib Husain, Dr. Eakramuddin, "Issues and challenges of admissibility of digital evidence: A study" 8(6) *IJNRD* (2023).

²⁰ Rahul K. Bharati, Pragati G. Khodke, Chaitali P. Khadiolkar, Dr. Shobha K. Bawiskar, "Forensic bytes: Admissibility and challenges of digital evidence in legal proceedings" 11(16) *International Journal of Scientific Research in Science and Technology* 24-35 (2024).

²¹ Dr. Pratyusha Das, Pradeepta Sarkar, "The importance of Digital Forensics in the admissibility of digital evidence" 7(2) *NUJS Journal of Regulatory Studies* 60-75 (2022).

of legal clarity on the constitutional position of metadata as a personal information.

At the constitutional level, the key development is the Supreme Court's judgment in the case of *Justice K.S. Puttaswamy v. Union of India*,²² which recognized the fundamental right to privacy under Article 21. In the judgment, it was clearly stated that any violation of the right to privacy by the state will have to pass the test of legality, legitimate state purpose, necessity and proportionality. In other words, the state cannot engage in surveillance on the pretext that it is convenient for the state. The judgment was also critical of the fact that secret surveillance is always prone to arbitrariness.²³ Although the judgment in *Puttaswamy* was not specifically on metadata, the judgment is relevant to the issue at hand.

The legislative foundation for communication surveillance in India was previously Section 5(2) of the Indian Telegraph Act, 1885, where it was stated that “*interception may be made on the occurrence of a public emergency or in the interest of public safety*” with a necessary condition that such action was taken on certain grounds such as sovereignty, security of State, maintenance of public order, or prevention of incitement to the commission of any offence. Although this provision was originally applicable to telegraph communications, it was the foundation for telephone interceptions in India for many decades. However, it was subject to significant influence from a Supreme Court judgment in a case titled *People's Union for Civil Liberties v. Union of India*,²⁴ where it was held that telephone tapping was a violation of privacy.

To achieve this, a new rule, namely, Rule 419A, was added to the Indian Telegraph Rules, 1951. This rule

specifically stated that such orders for interception are to be issued in general by the Home Secretary of the Union or State Governments, with a few exceptions in emergency situations, and are to be reviewed by a Review Committee.²⁵ Although this rule seems to have incorporated a system of checks and balance, it still remains largely an executive system as it remains within the executive domain to both issue such orders and review them.²⁶ There is no need for judicial approval for such interceptions, nor is there a robust system of post-surveillance notice, audit, or adversarial scrutiny by the affected party. This system assumes particular concern when it comes to metadata, as it is often accessed on a more routine basis with less visibility.

Correspondingly, there is a parallel basis under Section 69 of the Information Technology Act, 2000, which empowers the Central or State Government to issue a directive for the interception of information, monitoring of information, or the decryption of information generated, transmitted, received or stored in a computer resource if it is necessary or expedient on grounds similar to those of the Telegraph framework.²⁷ This setup is further fleshed out by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, which outlines the procedure for the issue of such directives.²⁸ This framework is particularly relevant in the current digital communication scenario since a considerable portion of metadata, IP addresses, login information, browsing information and other identifiers fall within the digital communication sphere regulated by the Information Technology Act.²⁹ However, again, this basis is not free of the same essential flaw.³⁰

²² AIR 2017 SC 4161

²³ Renu Rani, “The Right to Privacy in the Era of Mass Surveillance in India: A Constitutional Perspective” 6(4) *Journal of Humanities and Education Development* 47-54 (2024).

²⁴ AIR 1997 SC 568

²⁵ See r 419A, Indian Telegraph Rules, 1951.

²⁶ Bedavyasa Mohanty, “Inside the Machine: Constitutionality of India's Surveillance Apparatus” 12(2) *Indian Journal of Law and Technology* (2016).

²⁷ See s 69, Information Technology Act, 2000.

²⁸ See Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

²⁹ Ayush Panwar, “Network Interception and its Legal Issues” *SSRN* (2014).

³⁰ Jhalak M. Kakkar, Nehmat Kaur, Sharngan Aravindakshan, Shashank Mohan, Shubhi Agarwal, Sravya Movva, Vasudev Devadasan, Vrinda Bhandari, “The surveillance law landscape in India and the impact of Puttaswamy” *Centre for Communication Governance, NLU Delhi Press* (2023).

The problem with the Indian legal system is that it does not make a clear distinction between content data and metadata, although the constitutional implications of the latter can be significant. The law seems to view the issue of surveillance as a question of “interception” or “monitoring” broadly, without making a particular mention of metadata. This is a significant gap in the law. In the past, when the technology was different, it was perhaps reasonable to presume that non-content data was not problematic. But, this is no longer the case. The modern metadata allows for the identification of social networks, movements, political affiliations, religious practices, and individual habits with a reasonable degree of accuracy.³¹ The lack of a particular law on metadata means that the issue remains in a grey area, although the privacy concerns may be significant.³²

The existence of a reliable surplus statute is absent in India, which is another area of concern. The existing surveillance practices are based on a variety of sources including colonial telecom legislation, regulatory guidelines, digital communication legislation and industry-specific practices. As a result, there is a lack of a coherent legal basis for access with limited accountability via normative architecture. There is no central legislation that provides guidance for the following:

- a) when it is possible to access metadata,
- b) for which types of criminal behaviour it is applicable,
- c) the level of probable cause necessary for access,
- d) for how long data is allowed to be retained, or

- e) what type of review must occur prior to the access of the metadata.

The absence of these pieces has constitutional implications since any law that limits individual privacy is a violation of the constitution if it is not all of the following: clearly defined, predictable, and has procedures for enforcement.³³

The position is further complicated by the evidential aspect of criminal procedure. In fact, the Indian courts have displayed a willingness to accept illegally collected surveillance evidence, provided the relevance is established.³⁴ Such a position undercuts the deterrent effect of the rules, since the evidential value of the surveillance will be accepted regardless of the illegality of its collection.³⁵ Such a position appears to focus on the utility of the outcome rather than the legality of the procedure itself, which is a worrying aspect in the post-*Puttaswamy* era. In substance, therefore, the existing law in India is not that it prohibits metadata surveillance but that it allows it without any real thought or regulation.³⁵ What has been created is a regime where metadata is highly useful for criminal investigations but is not constitutionally or legally protected.³⁶ The ambiguity of the law is the central concern of the present paper. If privacy is to be taken seriously in the digital age, then metadata must not continue to be treated as a form of information that is constitutionally irrelevant or of secondary concern.³⁷ It must be integrated into a more coherent regime of legality.

³¹ J. Reddy, “The Central Monitoring System and Privacy: Analysing India’s Telecommunications Metadata

Interception” 20(3) *Indian Journal of Law and Technology* 55-78 (2014)

³² Gautam Bhatia, “State Surveillance and the Right to Privacy in India: A Constitutional Biography” 26(2) *National Law School of India Review* 127-162 (2014).

³³ Faheem Muhammed & Samarjit Kachari, “Surveillance, Privacy and the Policy Challenges: Decolonizing Personal Data Protection in India” 10(3) *Journal of Digital Media & Policy* 105-133 (2025).

³⁴ Jai Anant Dehadrai, Udipto Koushik Sarmah, “Surveillance, Criminal Investigations and Admissibility of Illegally Obtained Evidence: The Operationalisation of Privacy Post K.S. Puttaswamy”

SCC Times (19 October 2022). ³⁶ Ashwini Vaidialingam, “Authenticating Electronic Evidence: §65B, Indian Evidence Act, 1872” 8 *NUJS Law Review* 42-65 (2015).

³⁵ Naman Jain, “Admissibility of E-Evidence in India: An Overview” *SSRN* (2021).

³⁶ Vrinda Bhandari & Karan Lahiri, “The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World” 3(2) *University of Oxford Human Rights Hub Journal* 15-46 (2020).

³⁷ Devansh Malhotra & Rohit Kumar Shrivastava, “Bytes and Rights: Unpacking Search and Seizure of the Electronic Evidence Under India’s Legal

IV.POST-PUTTASWAMY JUDICIAL POSITION: CASE ANALYSIS AND CONSTITUTIONAL TENSIONS

A. *Judicial analysis of metadata surveillance*

In the years after *Puttaswamy*, Indian courts have changed how they deal with state surveillance, especially when it comes to using metadata in criminal investigations. Now, courts see metadata as more than just technical data. They see it as information that can show private parts of a person's life that are sensitive.³⁸ This acknowledgement has necessitated judicial scrutiny of surveillance practices to ensure compliance with constitutional criteria, particularly regarding legality, necessity, and proportionality. Judicial reasoning reveals several recurring themes that demonstrate how courts reconcile investigative requirements with privacy safeguards.

- a) One key focus of the judiciary has been the recognition of privacy as a fundamental right. The *Puttaswamy* judgment explicitly extended constitutional protection to personal data, making it clear that even non-content information like metadata can expose intimate aspects of life.³⁹ Courts have noted that any surveillance activity, including metadata collection, must be justified by law, necessary for a legitimate purpose, and proportionate to the intrusion.⁴⁰
- b) Another point of analysis is the legality of metadata collection. While laws such as Section 5(2) of the Indian Telegraph Act, 1885, and Section 69 of the IT Act, 2000, provide statutory

authorization, these provisions were designed before the digital age and do not specifically address the collection and analysis of metadata. Courts have pointed out that relying solely on broad executive powers is insufficient. Surveillance must have a clear statutory foundation that specifies scope, purpose and limits.⁴¹

- c) The principles of necessity and proportionality further guide judicial scrutiny. Metadata collection should be strictly tied to legitimate investigative objectives, such as serious criminal inquiries. Bulk or indiscriminate collection without individualized suspicion is increasingly viewed as constitutionally problematic. The judiciary insists that the degree of intrusion must align with the gravity of the threat, preventing excessive surveillance that could compromise personal freedom.⁴²
- d) Courts have also stressed the importance of oversight and procedural safeguards. While Rule 419A of the Telegraph Rules and the IT Rules provide some internal executive review, the lack of prior judicial authorization and limited transparency raises concerns about arbitrary surveillance. Judges have suggested that independent monitoring, auditing, and post-surveillance notice are essential to ensure accountability and protect constitutional rights.⁴³
- e) Finally, judicial analysis considers the evidentiary use of metadata. Metadata can provide vital leads and corroborative evidence, but courts emphasize that its value depends on lawful collection and contextual interpretation. Evidence obtained through unconstitutional or improper surveillance may trigger remedies, signaling the judiciary's

Framework" 4(1) *NFSU Journal of Forensic Justice* (2025).

³⁸ Samyukta Ramaswamy, "The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State" 20(2) *Indian Journal of Law and Technology* (2024).

³⁹ Faheem Muhammed, Samatjit Kachari, "Surveillance, Privacy and the Policy Challenges: Decolonizing Personal Data Protection in India" *Journal of Digital Media & Policy* (2025).

⁴⁰ Akshat Jain & Ayush Anand, "Tracing the Constitutional Journey of Data Privacy in India: From

Puttaswamy to the Draft DPDP Rules, 2025" *SSRN* (2025).

⁴¹ P Arun, "Power to Intercept, Monitor and Surveil: Cybersurveillance and Democracy in India" 13(1) *National Law School Journal* 108-138 (2015).

⁴² Rudraksh Lakra, "Notes from a Foreign Field: Ninth Circuit Court of Appeals and Bulk Metadata Surveillance" *Constitutional Law and Philosophy* (2020).

⁴³ A R Aksietha, "Surveillance in India and its privacy challenges in the digital age: A legal and constitutional analysis" 10(3) *International Journal for Research Trends and Innovation* (2025).

commitment to procedural integrity even when the evidence is relevant to criminal prosecution.

B. *Constitutional tensions arising from Metadata surveillance*

The growing use of metadata in criminal investigations has given rise to several constitutional conflicts, which have been focused upon by the courts in post-Puttaswamy case law.⁴⁴ Metadata, though considered a secondary or ancillary form of information, can convey detailed information on an individual's personal activities, social links and movements. The courts were faced with the complex issue of striking a balance between the interest of the State in criminal investigation and an individual's basic right to privacy.⁴⁵

The main balance to be struck is between privacy and investigative efficiency. Metadata allows law enforcement agencies to trace social networks, identify patterns, and track movements with great accuracy. It has thus become essential for effective investigations.⁴⁶ However, it also allows for a significant invasion of privacy. There have been observations that, while allowing for such efficiency, there cannot be arbitrary or mass surveillance. The invasion of privacy must thus be proportionate to what is necessary.

The other tension is based on the content and metadata dichotomy. Traditionally, the law has been more concerned with the interception of content than with metadata. However, the post-Puttaswamy case has challenged this view because the courts have realized the importance of metadata. The dichotomy between content and metadata could undermine the privacy rights of citizens and the constitutional framework.

The other issue that the courts have pinpointed is the balance between the executive and judicial oversight. The current framework gives the executive the power

to approve the collection of metadata with internal review but without judicial oversight. However, the courts have emphasized that the approval of the executive is not enough to satisfy the constitutional framework, especially when the surveillance is on a mass scale.

Lastly, there is a balance between admissibility of evidence and the protection of rights. For instance, metadata plays a significant role in criminal investigations. But, there has been a warning against normalizing metadata collection without reference to constitutional rights. While metadata evidence may be admissible, there are legal procedures to be followed in its collection, as seen in the judiciary's attempt to balance investigatory needs with the protection of fundamental rights.

V. CRITICAL ANALYSIS

In spite of the constitutional protection of privacy under *KS Puttaswamy v. Union of India*,⁴⁷ the Indian law on metadata surveillance is still wanting. The existing laws, such as the Telegraph Act, IT Act, and their regulations, have provided a wide scope for metadata collection by the State, but there is a lack of proper delineation of the scope for a rights-based approach. There is a state of authorization, but protection for privacy is still wanting. The courts have held that metadata is not merely technical information, but it is capable of reconstructing an individual's life, whereas metadata is still a secondary area, creating a structural imbalance between State power and individual rights.

The second important issue is the absence of prior judicial authorization. Although Rule 419A and the IT Rules provide for executive-level control, the absence of independent judicial authorization is a problem for the principles of necessity and proportionality. The concentration of surveillance power in the hands of the executive is a potential for abuse, especially in the context of political dissent, minority groups, or the

⁴⁴ Arushi Gupta, "The Case Against the Constitutional Validity of Mass Surveillance Programmes" 3(2) *Indian Law Review* 225-253 (2019).

⁴⁵ Faheem Muhammed, Samarjit Kachari, Surveillance, Privacy and the Policy Challenges:

Decolonizing Personal Data Protection in India 10(3) *Journal of Digital Media & Policy* 105-133 (2025).

⁴⁶ Parmy Olson & Mike Masnick, Metadata and the Constitutional Right to Privacy 31(4) *Communications of the ACM* 32-34 (2020).

⁴⁷ AIR 2017 SC 4161

investigation of crime. The judiciary has suggested that the collection of metadata could violate Article 21, although no mechanism is provided for its authorization.

Thirdly, the limits of metadata surveillance are still unclear with regard to the nature of the offense for which the collection is conducted and the period of time for which the information is stored. The courts have continuously cautioned against the collection of metadata on a bulk basis, but in reality, the agencies are able to access the information with minimal transparency. The balance between expediency and the rights of citizens continues to remain unaddressed with the system favoring expediency.

Another significant challenge that needs to be addressed is the ever-increasing rate of evolution of technologies, for which the legal system fails to catch up. With the advent of contemporary communication technologies, cloud computing, and AI-based analytics tools, there is a possibility of collecting a huge volume of metadata, much higher than what was contemplated in the Telegraph Act or IT rules. There have been apprehensions raised by courts that the current legal system is technologically outdated, with many provisions dating back to centuries ago. This has created a sense of ambiguity for both parties, as there are chances that metadata collection may result in a violation of constitutional provisions due to a failure to recognize contemporary technologies. Thereby, without a specific recognition of technologies, there are chances that the State may exercise powers that are legally valid but constitutionally questionable.

More concern, however, lies in the lack of transparency and accountability in metadata surveillance. There is a lack of information to citizens regarding the collection, analysis, or storage of their metadata. There are also few reporting requirements for the executive. In fact, it has been observed by courts that “surveillance conducted in secret can erode trust in government and foster a sense of potential misuse.” In contrast, comparative jurisprudence indicates that periodic reporting requirements are an essential component of ensuring that metadata surveillance does not become arbitrary or unreasonable. In the absence of such requirements, the legal framework leaves the executive to function in a

dark space, which may not be in consonance with the constitutional guarantee of privacy under Article 21.

Finally, the admissibility of metadata evidence points to another gap in this context. In India, for example, evidence gathered through improper procedures is deemed admissible as long as it is relevant to the investigation. Although this is helpful for law enforcement agencies, this practice also promotes a culture of disregard for privacy, which is against the constitutional principles set out in the judgment in *Puttaswamy*.

Thus, it can be asserted that the critical analysis of the topic has shown how, despite the recognition of the right to privacy as an essential right by the Indian judiciary, the framework and checks with regard to metadata surveillance are not adequate. It is a grey area, and the balance between its utility and constitutional integrity is tilted towards the convenience of the state. Reforms are the need of the hour if the concept of privacy is to hold substantive meaning in Indian criminal jurisprudence.

VI. RECOMMENDATIONS

In order to bridge the gap identified with the use of metadata surveillance, the *first* step is the enactment of a special law on the subject of metadata collection. The Telegraph Act and the Information Technology Act are not adequate on the subject of metadata collection because they are old and have not clearly defined the concept of metadata or its collection. A special law on the subject must clearly define the concept of metadata and its collection in order to strike a balance between the investigative agencies and the Constitution. It must clearly define the purposes for which metadata collection is permissible and the limits of collection.

Secondly, there is a need for institutionalized judicial oversight for all metadata surveillance activities. There is a necessity for prior judicial authorization for metadata collection, particularly when there is a question of bulk or prolonged monitoring. There is a need for courts to have a role in assessing necessity, proportionality and possible intrusiveness before metadata is accessed. This would be a direct response to the issue of arbitrary executive action, which is a concern, and would put India on par with global best

practices, which emphasize independent oversight as a key feature of rights-friendly surveillance.

Third, the principle of proportionality and purpose limitation is essential in the collection of metadata. In this regard, the investigators should only collect the metadata that is directly related to the investigation. In addition, the investigators should limit the amount of metadata collected, excluding excessive metadata that is not related to the investigation. Finally, the retention period for the metadata collected should be limited, thus creating a mechanism for reviewing the metadata to ensure that it does not become a permanent repository for the personal information.

Fourth, transparent reporting and accountability measures need to be implemented. Agencies that are undertaking the surveillance need to make transparent reports on the number of requests made, approvals granted, and justifications for such approvals. There also needs to be auditing to ensure that there is compliance with legislative and constitutional provisions. This will ensure that there is increased trust in the system and that there are no perceptions of secrecy.

Fifth, given the rapid evolution of digital technologies, there is an urgent need for technologically informed regulations. Laws should account for AI-assisted analytics, cloud storage, and crossplatform data aggregation, providing clear guidance on how these innovations intersect with privacy rights. Regulators should collaborate with technology experts to ensure legal standards remain relevant and enforceable in the face of evolving digital threats and investigative tools.

Finally, to protect procedural integrity, evidentiary standards for metadata must be codified. Courts should only admit metadata that has been collected lawfully and under proper authorization, with mechanisms to challenge unauthorized access. Clear procedural safeguards will ensure that privacy rights are respected while maintaining the evidentiary value of metadata in criminal investigations.

Collectively, these measures would create a balanced legal basis where metadata serves legitimate criminal investigation needs without compromising the constitutional right to privacy, offering a roadmap for

India to reconcile security with individual liberty in the digital age.

VII. CONCLUSION

In an era where the digital footprint leaves the deepest secrets of life exposed, metadata is certainly not the “merely technical information” it used to be. The post-*Puttaswamy* case law shows the fact that privacy is a fundamental value of the Constitution, and even the least suspicious of information cannot escape judicial review. The Indian judicial system has sought to strike a precarious balance between the ability of the law enforcement agencies to use metadata for the purpose of investigation and the risk of the State descending into surveillance. However, the present law is inadequate and piecemeal, reflecting the pre-digital era statutes, leaving citizens vulnerable and the courts to fill the gap.

This research shows that the balance between investigation efficiency and fundamental rights is not merely a theoretical problem. It actually has practical consequences in terms of procedural gaps, technological uncertainties and obscure executive powers. The value of metadata as evidence does not justify a breach of the fundamental right to privacy, although judicial creativity has to a certain extent compensated for outdated legislative provisions. The path forward is one in which there is a comprehensive and forward-thinking approach to legalizing metadata, mandating judicial review, incorporating proportionality in collection, technological flexibility, transparency and codified rules for evidence. In this way, India can move from a position in which metadata is a potential mechanism for intrusion to one in which it is a mechanism for justice, security, and liberty.

Ultimately, the new test for privacy after *Puttaswamy* is not only a legal test but also a

philosophical test: how to ensure that in the pursuit of safety and efficiency, the right to privacy is maintained as a non-negotiable core principle of a free and democratic society. Metadata, if used properly, can be a powerful tool in an investigation. Metadata, used improperly, can quietly undermine the freedoms that the Constitution is meant to protect.