THE LEGALITY OF TELEPHONE TAPPING AND INTERCEPTION: A STUDY WITH REFERENCE TO FUNDAMENTAL RIGHTS

Aarti Sharma, B.A. LL.B. (Hons.), Law College Dehradun, Uttaranchal University

Dr. Abhiranjan Dixit, Associate Professor, Law College Dehradun, Uttaranchal University

ABSTRACT

This article critically examines the legal and constitutional framework governing the interception of telephonic and digital communications in the Indian legal system. At the very onset of this study is to analyse the permanent tension between the sovereign's mandate to ensure national security and the citizen's fundamental right to privacy, which is now unequivocally protected under Article 21 following the landmark judgement in the case of *K.S. Puttaswamy*. While tracing the historical evolution from the colonial era statute of the Indian Telegraph Act, 1885, to the recently enacted Telecommunications Act, 2023, the research highlights an everlasting legislative reliance on broad, undefined thresholds such as "public emergency" and "public safety." Furthermore, the study analyses the differences and unequal statutory treatment of traditional voice telephony versus digital surveillance under Section 69 of the Information Technology Act, 2000.

By evaluating post *PUCL* jurisprudence and the evidentiary admissibility of intercepted communications under the new Bharatiya Sakshya Adhiniyam, 2023, the paper exposes the structural vulnerabilities of relying exclusively on an internal executive Review Committee. Ultimately, the article tries to argue that in order to satisfy the constitutional test of proportionality and prevent a chilling effect on the freedom of speech, India urgently needs a transition from an *ex-post* executive review system to a framework mandating independent, *ex- ante* judicial authorization for state surveillance.

INTRODUCTION

In day-to-day life phone plays a very ordinary and important role as a means of communication. Phone tapping is a very serious offence that infringes privacy of an individual. In India, the power to intercept phone calls is not unconditional, and it is one of the essential measures regarding national security, provided it is exercised in accordance with the law. The Legislative aspects of the problem are to strike out the balance between the sovereign interests of the state and the fundamental rights of citizens in terms of Article 19(1)(a) [right to freedom of speech and expression][1] and Article 21[right to life and liberty][2]. The telephone tapping of an individual's conversations or communications, that may be with or without his knowledge and consent, may amount to a serious infringement of his right to privacy. The courts have stipulated conditions and have also provided safeguards in accordance with the statute to be complied with from time to time in this regard, to prevent the infringement of citizens' fundamental rights. The practice and concept of telephone tapping has surely come a long and chequered history, while the legislative provisions are based on the Indian Telegraph Act,1881. However, the practice and concept of telephone tapping have undergone a sea change and significant development, especially after judicial intervention in this regard.

HISTORICAL EVOLUTION OF INTERCEPTION LAW IN INDIA

Historical development of telephonic interception in India is essentially bound to the colonial jurisprudence, in particular to the period of the law such as the Indian Telegraph Act of 1885 which was mainly written to bring the administrative control of Britain together and observe dissent in the course of the revolution, Section 5(2) of the Indian Telegraph Act of 1885[3] allowed the executive to have a sweeping and mostly unrestricted authority in intercepting communications. These powers were subject to the invocation on two broad and statutorily undefined preconditions, the first of which was the presence of a public emergency or measures undertaken in the interest of public safety. Among the most outrageous ones was the fact that despite decades that had passed since the independence, this colonial system structure was still present in our system and was frequently utilized with little to no legislative control. Pre-emergence judicial interpretations were characterized by the propensity to give large degrees of deference to executive judgment, in consideration of which the evaluation of an emergency

[1] Constitution of India
[2] Constitution of India
[3] Indian Telegraph Act of 1885

situation by the state was regarded as non-justiciable. This historical deference left a large disparity, with the imperatives of state security always preeminently rolling over the individual considerations of privacy, and finally requiring subsequent constitutional readings to reinterpret into a fundamentally authoritarian statute the democratic guarantees.

THE CONSTITUTIONAL FRAMEWORK AND THE BASIC RIGHTS.

The jurisprudential transformation of Articles 21 and 19 in Part III of the Constitution of India is inherently bound to the constitutional legitimacy of telephonic interception in India. Earlier on, the border between state surveillance and individual freedom has always been full of ambiguity as it is currently clearly depicted by the precedent set by Kharak Singh v. State of U.P.[4] and Gobind v. State of M.P.[5], in which the right to privacy was acknowledged only peripherally and conditionally and not entirely. But this paradigm changed forever with the historic nine-judge bench ruling, K.S. Puttaswamy v. Indeed, in the case of Union of India (2017)[6], privacy was clearly made an intrinsic aspect of the right to life and personal liberty in Article 21 under union of India. Any executive order requiring interception has now to pass the stern test of the doctrine of proportionality, or an order violating that doctrine is against the principle of natural justice. This requires that they meet a specific threshold, and that the act must be authorised by a lawful statute which will ultimately serve a legitimate state interest (national security), and that such a nexus is rational and proportional, such that infringement is the minimally restrictive action which may be taken. Moreover, the intrinsic character of telephone tapping is the first violator of Article 19(1)(a) that produces an overwhelming chilling effect on the freedom of speech and expression. No such power of state surveillance can therefore exist in a space; it must be carefully weighed against these core rights and can only be justified when falling well within the very restricted constraints of the category of reasonable restrictions contained in Article 19(2) of the Indian Constitution.

COURTS OF LAW AND CASES

The landmark case in Indian surveillance legislation was the Decision of People's Union for Civil Liberties (PUCL) v., which defined the jurisprudential watershed of this law. Union of India (1996). It is this same case that faced the popular claims of politically motivated

[4] Kharak Singh v. State of U.P. 1963 AIR 1295, 1964 SCR (1) 332
[5] Gobind v. State of M.P 975 AIR 1378, 1975 SCR (3) 946
[6] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1 or AIR 2017 SC 4161

telephone tapping, and the Supreme Court realized that although Section 5(2) of the Indian Telegraph Act[7] could not be invalidated wholesale on the grounds of sound state security concerns, the unbridled application of it could not be considered as constitutional. The Court upheld the fact that telephonic conversations come close to the spectrum of right to privacy in Article 21. In a quest to heal the statutory vacuum of the procedural protections, the Supreme Court undertook extraordinary measures to provide broad guidelines, by dictating that interception orders would only be made by the supreme executive of the nation, namely, that of the Home Secretary of the Central or State Government.

These judicial instructions were then formalized into Rule 419A of the Indian Telegraph Rules, 1951[8], to make a broad executive declaration into a formal procedural format.

Under rule 419A, there were now important protective measures, such as regular time restrictions on interception orders, the maintenance by the police of logbooks, and the destruction of intercepted material not pertinent directly to the investigation. Assuming we observe, Crucially, that it has put in place a Review Committee that is constituted of senior bureaucrats such as the Cabinet Secretary, Law Secretary, and Telecommunication Secretary, whose role is to determine the legality of interception orders within a period of sixty days. This was a specially authorized committee that could effectively recall orders and require intercepts that could not meet the criteria of the public emergency or public safety levels to be demolished.

THE MODERN STATUTORY REGIME: A CRITICAL ANALYSIS

Switching to the Telecommunications Act, 2023: How did it change? The passage of the Telecommunications Act, 2023, which officially repealed the Indian Telegraph Act of 1885 of the colonial period, was expected to be one of the watershed events in the modernization of the Indian privacy and surveillance system. Nonetheless, a legal critique demonstrates that the new law does little but put the old wine in a new bottle when it comes to state surveillance and is not as efficient as it can be. Looking at Section 20(2) of the 2023 Act, controlling interception of messages, it has retained the same substantive thresholds as that of its predecessor: interception is only allowed to happen when a public emergency occurs, or for the safety of the public. Although the Act is complemented by the recently announced Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 (the

[7] Indian Telegraph Act 1885
[8] Indian Telegraph Rules, 1951

replacement of the PUCL-inspired Rule 419A), the inherent issue is that the legislature failed to take an important step of legally defining what a public emergency should be. Keeping this threshold unspecified, the law still allows the executive broad discretion in its interpretation. The operational safeguards are formalized in the 2024 Rules, because we find that it can be used by the head of an authorized agency to issue orders in remote emergencies or operational emergencies (as long as the Competent Authority (the Home Secretary) confirms it in a duration of seven days) but what actually occurs is that the substantive core of the surveillance power is identical to the 1885 regime.

The Information Technology Act 2000 (Section 69) vs. telecommunications laws. A significant source of tension in contemporary Indian surveillance jurisprudence is the fact that there is a dualistic legal regime. Though the traditional voice telephony is regulated by the strict Telecommunications Act criteria of the public emergency, the interception of digital data, over the internet, and encrypted communications is directly regulated under the Information Technology (IT) Act, 2000, Section 69.

In this way, it has generated an anomaly in statutory law. In the IT Act, Section 69, we find that it makes no reference to a prerequisite of a public emergency or public safety. Rather, it expands the authority of the state, giving it the power to investigate any offence. This means that law enforcement is able to intercept an email or even an internet-based message with a much lower threshold than a normal cell phone call. This two-track system poses some real constitutional issues about the equal protection of laws as stipulated in Article 14 because the level of protection of privacy that is granted to an individual citizen in reality relies on the medium through which communication happens and not on the nature of the threat.

COMPETITIVE INTERNATIONAL VIEWPOINTS.

The United States: The Fourth Amendment, Warrants, and the FISA Courts. The United States undertakes the investigation of communications in a very strict constitutional approach, the Fourth Amendment of the Constitution, which provides a shield against unreasonable searches and seizures to the very nature of a citizen. The law of US surveillance in the modern world is based on the jurisprudential foundations of the Supreme Court ruling in the well-known case of Katz v. In the United States (1967), which popularly stated that the Fourth Amendment only protecting individuals, and not property, the reasonable expectation of privacy test in the context of telephonic conversations. In turn, Title III of the Omnibus Crime Control and Safe

Streets Act of 1968 (the Wiretap Act) regulates domestic wiretapping in the US and requires the presence of an ex-ante judicial warrant. The police are required to prove to a neutral federal judge that it has a reasonable probable cause before actually intercepting domestic communications.

The system is regulated in regard to foreign intelligence collection through the Foreign Intelligence Surveillance Act (FISA) of 1978. Although FISA permits more covert operations, it must be authorized by a special, independent judicial organization, the Foreign Intelligence Surveillance Court (FISC). Despite the high volume of criticism that has been leveled at the FISC as a rubber stamp, the difference between the structure of the Indian system and that of the US system is that the power to issue the authorization is squarely in the judicial branch and not the executive branch, like in India.

The Standards of the United Kingdom and the European Court of Human Rights (ECHR) Surveillance system in the United Kingdom is intricately connected to the jurisprudence of the European Court of Human Rights (ECHR), namely Article 8 of the European Convention on Human Rights that provides the right to respect to family and personal life. As part of a reaction to rulings by the ECHR that highlight the necessity of stringent oversight (as was in Big Brother Watch v.). In the UK, the Investigatory Powers Act 2016 (IPA) was enacted by the UK.

Although the IPA provides the intelligence agencies with a great deal of surveillance abilities, it also provides a procedural protection called the Double Lock mechanism.

In the case of the Double Lock, a Secretary of State (the executive) has to first issue an interception warrant. The warrant, however, cannot be enforced until it is reviewed and approved by a Judicial Commissioner, who is a senior judge acting under the Independent Investigatory Powers Commissioner office (IPCO). The Judicial Commissioner applies judicial principles of review to determine the necessity of the warrant and whether it is, in fact, proportionate to do so. It is this hybrid model that has been able to bring together the intelligence expertise of the executive and the independent judicial scrutiny.

CONCLUSION

Legal provisions that regulate telephone tapping and electronic surveillance in India are an

indication of a balance between national security and individual freedom that is still being adjusted, though it has not been optimally achieved. As this paper will demonstrate, the replacement of the Indian Telegraph Act of 1885 by the more comprehensive Telecommunications Act of 2023 was a great opportunity to make state surveillance capabilities correspond to the right to privacy as recognized in the case of K.S Puttaswamy. However, the existing law system has not changed much to address the major gaps that existed in the previous system. The use of imprecise terms like the term of public emergency and the inconsistency and injustice of the different standards used between the traditional telecommunications and digital interception in the IT Act, 2000, and the total reliance on an executive Review Committee are indicative of a reluctance on the part of lawmakers to put the

use of surveillance into a full review under the constitution. The current system fails the proportionality test because structural safeguards against too much executive power are absent, having a chilling effect on the freedoms in Articles 19(1) (a) and 21.

The most evident constitutional copy in the interception system of India is that there is no pre-approval judicial control in it, as is perceived in the United States of America. The Review Committee mechanism that is established is based on an incorrect paradigm of Caesar judging Caesar, which goes against the doctrine of separation of powers. Executive bureaucratic review, which is post-facto, cannot structurally deliver the much-needed impartial, rigorous examination needed to warrant a severe invasion of fundamental rights. The comparative study of the constitutions of different countries, such as the United States and the United Kingdom, highlights that efficient surveillance does not necessarily go against efficient judicial control. The authority to intercept should be independent of the investigative and executive power to avoid arbitration of power and to make sure that the intrusions of the state are necessary and even relevant.