IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ADMISSIBILITY OF SURVEILLANCE EVIDENCE AND SURVEILLANCE LAW IN INDIA

Mohammad Elham Khan

Amity Law School, Amity University, Lucknow, Uttar Pradesh, India

Abstract: Surveillance is a valuable instrument for upholding societal order and ensuring national security. However, when carried out by unauthorized individuals or third parties, it can pose significant challenges for the general population and potentially compromise the nation's well-being. For example, the aforementioned instances of illegal tape cases demonstrate how targeted individuals, who hold critical roles within the country, become vulnerable to privacy breaches. Such illicit monitoring or snooping activities can consequently pose a threat to national security and integrity. In the current context, it is imperative that the government take a more stringent approach to data protection and safeguarding the rights of its citizens. Political interests drive governmental entities to occasionally infringe upon individuals' fundamental rights and engage in actions deemed unreasonable, as exemplified by the Peagasus case. This raises the question of whether third parties or individuals are also capable of committing similar transgressions.

Index Terms **- Surveillance, illegal, evidence, security, Puttaswamy, Supreme court.**

I. INTRODUCTION

Surveillance refers to the act of systematically observing, gathering, or intercepting information pertaining to an individual by a party other than the individual in question. Given the rapid progress of technology and the growing population of telecommunication and internet consumers in India, there is an elevated risk of individuals inadvertently disclosing personal and confidential information through these prevalent modes of communication. However, it is important to recognise that the transmission of such data may be susceptible to interception and monitoring by unauthorised third parties. In order to mitigate such circumstances, India has previously implemented legislation pertaining to the surveillance of phone calls or websites. Surveillance, when implemented strictly, can serve as a valuable tool for monitoring national security and detecting criminal offences. In this regard, specific authorities and departments are granted the authority to monitor and intercept the data of individuals, provided that the reasons for doing so align with the stipulations outlined in relevant legislation [1].

Currently, in India, the oversight of surveillance matters is carried out through two legislations. The first one is the Telegraph Act of 1885, which primarily focuses on the interception of calls. This act prohibits any third party from intercepting calls and also establishes the authority and valid justifications for such interceptions. The legislation that pertains to surveillance is the Information Technology Act of 2000, commonly referred to as the IT Act of 2000. The legislation under consideration pertains to the monitoring and oversight of electronic communication, encompassing a range of measures aimed at establishing essential regulations and guidelines in this domain [2].

The topic of surveillance has gained significant attention in recent times, with the emergence of incidents such as the Peagasus scandal, where it is claimed that data belonging to several prominent individuals in India was tracked. This incident has prompted the government to reassess its policies about surveillance and take measures to prevent similar occurrences in the future. According to the Supreme Court of India, illegal

surveillance poses a significant and grave threat to the security of individuals. The court has observed that privacy is a fundamental right for every Indian citizen. The implication of a threat to privacy poses a significant risk to the fundamental liberties of netizens as enshrined in the Constitution of India. As part of ongoing efforts, the central government is currently engaged in the development of more comprehensive and refined legislation aimed at addressing cyber issues and safeguarding individuals' data. The proposal also includes a provision for the establishment of a Data Protection Authority. This authority would be responsible for addressing concerns related to data protection and privacy [1,2]

The escalating presence of surveillance in India is becoming increasingly concerning as the government continues to enhance its technological capabilities for monitoring citizens. However, what exacerbates the situation is the dearth of transparency and accountability surrounding these surveillance practices. Within the context of the continuing litigation before the esteemed Supreme Court of India, it has come to light that the Indian government has acknowledged its engagement in electronic surveillance activities. The 'Standard Operating Procedure', a previously undisclosed document that had not been publicly available until now, was the subject of this revelation [3]. The emergence of this phenomenon has raised concerns about the potential escalation of power concentration within the executive branch due to the secrecy surrounding covert surveillance efforts. The current state of the law is insufficient to guarantee the necessary level of accountability. Initially, it is important to note that the statutory prerequisites for legitimate surveillance are characterised by a broad and inclusive language, thereby affording the government a significant degree of flexibility in substantiating the legality of specific instances of surveillance. In India, the executive branch exclusively holds the authority to authorise and oversee surveillance activities. The absence of independent inter-branch oversight, such as parliamentary or judicial scrutiny, renders these decisions immune from external checks. Furthermore, there is no stipulation mandating the inclusion of the affected individual in the decision-making process, either prior to or subsequent to their placement under surveillance. Moreover, Indian law generally admits illegally obtained evidence in court proceedings, as long as it is considered relevant to the case. The aforementioned implications, specifically pertaining to the final two components—namely, the exclusive jurisdiction of the executive branch in granting surveillance authorization and the admission of unlawfully obtained evidence during legal proceedings—bestow upon the state an imbalanced and unrestrained authority to acquire and exploit personal data [4,5].

Within the framework of the aforementioned issues, it is imperative to consider and recognise the viewpoints of various other nations and endeavour to identify potential approaches for addressing third-party data interception. It is critical to consider the viewpoint of the esteemed Supreme Court of India, as well as the numerous directives and observations issued by the court.

II. HISTORICAL BACKGROUND OF SURVEILLANCE IN INDIA

India has experienced numerous instances of illegal surveillance, particularly in the realm of Indian politics. One notable instance of snooping involves the resignation of Ramakrishna Hegde, the former chief minister of Karnataka, in 1998. This decision was prompted by a scandal related to the unauthorised interception of telephone conversations. The individual in question resigned from his position based on ethical considerations subsequent to the disclosure of wiretapping activities targeting a total of 50 individuals, which included journalists and dissidents affiliated with the Janta party. Consequently, the disclosure of the authorization granted to the state police for conducting wiretapping activities was made publicly available [6]. Furthermore, it is worth noting that the detrimental consequences of illegal surveillance extend beyond mere implications. A notable instance occurred in March 1991, when two Haryana policemen were apprehended for engaging in unauthorised surveillance outside the residence of Rajiv Gandhi. This incident ultimately resulted in the resignation of the incumbent Prime Minister, Chandrashekhar. Expressing strong discontentment regarding the purported act of surveillance, Rajiv Gandhi made the decision to withhold his support for Chandrashekhar during the vote of confidence. The Tata Tapes, a well-known incident, represent a significant concern regarding illegal surveillance. The Tata tapes represent the initial occurrence of a significant leak involving a substantial number of intercepted conversations. These tapes specifically encompass discussions involving prominent industrialists such as Nusli Wadia, Ratan Tata, and Keshub Mahindra [7,8].

The wiretaps that were unlawfully disclosed by The Indian Express revealed Tata's endeavours to seek intervention from the central authority in a case involving the United Liberation Front of Assam (ULFA), which was engaged in extorting funds from tea estates, including those under Tata's ownership. Subsequent to the audio tape leaks, the then Prime Minister, I.K. Gujral, took the decision to initiate a CBI inquiry. However, it is worth noting that the inquiry was subsequently terminated due to insufficient evidence. Over a decade has passed since the Tata tapes, wherein numerous interactions of corporate lobbyist Nira Radia were

leaked in 2008. The income tax department meticulously recorded conversations of Radia, a prominent figure, with influential politicians, industrialists, and journalists over a span of 300 days from 2007 to 2009. This extensive documentation was conducted in relation to the 2G telecom scam. One of the individuals with whom lobbyist Niira Radia engaged in conversation was Ratan Tata. Subsequent to the public disclosure of these recorded conversations, Tata initiated legal proceedings in an effort to obtain an injunction preventing the media from disseminating any further recordings of this nature [7,8].

The issue of illegal surveillance has been a persistent concern throughout Indian history. The recent emergence of the Peagasus virus has raised questions about the efficacy of existing legislation on surveillance in India, thereby highlighting the urgent need for a revised and more stringent legal framework in this regard. The phenomenon of illegal surveillance has been identified as a significant and concerning menace to electronic communication, thereby posing a direct risk to the security and privacy of individuals. In addition to its implications for individual privacy, the use of personal data can also pose a significant risk to national security. Therefore, there is a growing need for more stringent legislation to address this issue [9].

III. INTERNATIONAL PERSPECTIVE

The regulation of surveillance poses significant challenges, prompting the establishment of diverse legal frameworks and regulatory bodies in developed countries. These frameworks may hold persuasive value when considering their applicability within the Indian context. Upon conducting an extensive analysis, it has been determined that there are several major countries that have implemented regulations on surveillance. These countries have recognised the importance of striking a balance between ensuring national security and protecting individual privacy rights [10]. The following countries have established specific guidelines and laws pertaining to surveillance practices:

United States: The United States has implemented various regulations on surveillance, primarily governed by the Fourth Amendment of the U.S. Constitution. The United Kingdom has implemented several laws to regulate surveillance. Among these laws, there are a few major ones that are worth mentioning:

- **The European Convention on Human Rights (ECHS)** is a legally binding international treaty that aims to safeguard the fundamental rights and freedoms of individuals. It places an obligation on the government to ensure the protection of these rights for its citizens. Article 8 of the relevant convention grants individuals the right to respect their private and family life, as well as their home and correspondence.
- **The Intelligence Services Act of 1994 (ISA)** is a legislative framework that establishes provisions for the issuance of authorizations and warrants, which enable intelligence services to undertake actions related to the interception of wireless telegraphy.
- **The Police Act of 1997**, specifically Part 3, outlines the provisions and justifications for authorising interference in an individual's property and privacy.
- **The Data Protection Act 2018** is a piece of legislation that governs the processing of personal data. Its primary goal is to guarantee the secure and lawful handling of individuals' personal information. The provision of regulations for effective information handling is a requirement that organisations must adhere to.
- **The General Data Protection Regulation (GDPR)** is a comprehensive piece of legislation that has been enacted across Europe. Its design aims to regulate the use and processing of personal information [11].

Russia: The Russian constitution guarantees the right to privacy as well as the protection of personal and family secrets. It also ensures that individuals have the right to keep their communications confidential, with any limitations requiring a court decision. The collection, storage, and use of an individual's personal data are only permissible with explicit consent from the concerned individual. In 2007, the Russian government implemented the Personal Data Law, which represented a significant legislative development in the realm of data privacy concerns. The implementation of data protection measures is crucial in order to safeguard various forms of data. Additionally, it serves the purpose of clearly defining the classification of private data as well as determining the permissible collection of data and the authorised entities responsible for such collection, subject to the consent of the relevant individuals. The Yarovaya Law, enacted in May 2014, exerted control over the Russian telecom and internet industries. According to the regulation, it has been mandated that all telecommunications companies are required to retain all voice and text messages for a period of six months. Furthermore, these companies are obligated to furnish the requested data to law enforcement authorities upon their request [10,11].

Australia: In Australia, the government has implemented specific legislation to regulate interception and surveillance practices. One such piece of legislation is the Telecommunications (Interception and Access) Act

of 1979. The Telecommunications (Interception and Access) Act of 1979 encompasses various provisions concerning the interception and storage of personal data, along with the criteria and circumstances that allow for its interception. The Surveillance Devices Act of 2004 is significant legislation in the legal framework of the Commonwealth of Australia. This act specifically addresses the use and regulation of surveillance devices within the country. The aforementioned act encompasses a set of powers that are designed to facilitate investigations conducted by the commonwealth within a restricted scope of criminal offences. These laws represent a few examples from various countries. It is important to note that many other countries have also enacted specific acts or legislation pertaining to surveillance. From an international perspective, it is evident that individuals have the right to maintain the privacy of their personal data and communications within their own country. Any form of surveillance or data collection that infringes upon this right is considered a violation of privacy. However, it is important to note that surveillance can also be a valuable tool when used in a legitimate manner. It can aid in the detection of threats to national security and a country's integrity. Many nations employ surveillance techniques to monitor and apprehend criminals, which assists relevant authorities in their efforts to detain them [12].

IV. INDIAN PERSPECTIVE

Surveillance in India has emerged as a significant concern in recent times, following the discovery of spyware known as Pegasus, which purportedly gathered data from approximately 300 individuals without their knowledge or consent. This incident has prompted the government to reevaluate its existing laws and policies pertaining to surveillance [13]. Presently, there are two primary legislations in India that address the issue of surveillance:

i. The Telegraph Act 1885

The Telegraph Act of 1885 primarily focuses on the regulation and control of telegraph communication, particularly with regards to the interception of telephone calls. The legislation in question pertains to the regulation and oversight of various forms of communication, including both wireless and wired telegraphy, radio, and digital data communications. The provision grants the government of India the authority to establish, maintain, operate, and supervise all forms of either wireless or wired communications within the geographical boundaries of India. Furthermore, it grants government law enforcement agencies the authority to engage in communication interception and phone line tapping, subject to the stipulations outlined in the Constitution of the Republic of India [14].

The legislation under consideration pertains to the interception of telephone calls. The primary provision governing this matter is Section 5(2) of the Telegraph Act. According to this section, if there is a public emergency, concerns regarding public safety, or if it is in the interest of the public, the central or state government, or any authorised representative acting on behalf of the central or state government, may intercept calls. Protection of India's sovereignty and integrity, ensuring national security, or preventing any criminal offences justify this interception. It is imperative to ensure that any message, including but not limited to those transmitted via telegraph, is documented in writing. Furthermore, it is crucial to prevent the transmission, interception, or detention of such messages, as well as to prohibit their disclosure to the government. [14,15].

This legislation grants the government the authority to monitor telephone conversations in specific circumstances, such as to safeguard national sovereignty and integrity. These restrictions align with the limitations placed on freedom of speech as outlined in Article 19(2) of the Indian Constitution. Besides the previously mentioned conditions, it's crucial to remember that lawful interception does not apply to journalists.

ii. Information Technology Act, 2000

The Information Technology Act of 2000 is the widely recognised legislation in question. This research focuses primarily on the study and analysis of cybercrime and its impact on electronic commerce. The formulated legislation aims to legalise transactions that involve digital interaction and information storage. The subject matter pertains to criminal activities that encompass the use of an electronic device or network situated within the geographical boundaries of India. Within the realm of surveillance, Section 69 of the Information Technology Act and the Information Technology Rules 2009 (Procedure for Safeguards for Interception, Monitoring, and Decryption of Information) were implemented to enhance the existing legal structure pertaining to electronic surveillance. According to the provisions of this act, it is permissible to intercept all electronic transmissions of data. In addition to the limitations outlined in the Telegraph Act and Article 19(2) of the Constitution, Section 69 of the IT Act expands the scope of surveillance by allowing its use in the investigation of criminal offences [10, 11 & 13].

In addition to the aforementioned enabling legislation, the government of India has implemented a bill known as the Personal Data Protection Bill, 2019. The proposed legislation aims to address the issue of safeguarding individuals' personal data by establishing a dedicated data protection authority. This authority

will be responsible for overseeing and enforcing measures to ensure the privacy and security of personal information. The proposed legislation aims to facilitate the processing of personal data by various entities, including the government, businesses founded in India, and foreign companies that handle personal data of individuals residing in India. Personal data refers to the category of data that, upon being processed or decrypted, has the potential to reveal an individual's identity or identification [11].

Currently, the aforementioned bill is undergoing analysis by a Joint Parliamentary Committee. Recent observations indicate that experts are expressing concerns that the Data Protection Bill is biassed towards the government and may divert attention from safeguarding individual privacy. The report of the Joint Parliamentary Committee has been officially adopted following an extensive two-year period of deliberation. Within this report, the committee has put forth a range of recommendations aimed at enhancing and refining the existing framework. Notably, one of the key proposals entails a revision of the nomenclature, specifically advocating for the alteration of the current name to 'Data Protection Bill', thereby omitting the term 'personal'. The report proposes that a unified regulatory body should oversee both personal and non-personal data. This approach is suggested as a means to ensure consistent and comprehensive oversight of data management practices across different types of data. By having the same regulator responsible for both personal and non-personal data, it is anticipated that there will be greater efficiency, coordination, and alignment in the regulation of data usage and protection. This recommendation is based on the understanding that personal and non-personal data are interconnected and that a holistic regulatory approach is necessary to address the complex challenges associated with data governance [11,13].

V. Judicial Approaches

The Supreme Court of India has extensively deliberated on the issue of unauthorised surveillance and its implications for the fundamental rights of citizens. Several noteworthy observations made by the Supreme Court include:

The Supreme Court (SC), in the case of Public Union for Civil Liberties (PUCL) vs. Union of India [16], made an observation regarding the absence of adequate procedural safeguards in the relevant sections of the Telegraph Act. Consequently, the court proceeded to establish specific guidelines pertaining to the interception of telephone calls. It is worth noting that the Supreme Court has observed that the relevant authorities have been found to be deficient in maintaining adequate documentation and records of the interceptions. The court's ruling highlights the recognition of tapping as a significant infringement on an individual's privacy. It emphasises the responsibility of government entities to safeguard an individual's right to privacy, which is currently being exploited by the authorities. In the recent legal proceeding of Manohar Lal Sharma vs. Union of India and Ors. [17], the focus was on the Peagasus spyware. This spyware has been accused of intercepting and monitoring the data of approximately 300 individuals in India.

The SC has recognised that individuals in a civilised democratic society possess a justifiable anticipation of privacy. It is imperative that every citizen of India be safeguarded against privacy infringements. This notion is supported by the landmark case of K.S. Puttaswamy v. Union of India [18], in which the SC affirmed that privacy is a constitutionally protected right. Specifically, it is deemed a fundamental right under Article 21 of the Indian Constitution. Furthermore, any legislation that impinges on an individual's privacy must adhere to the constitutional requirements for restricting fundamental rights. The SC has unequivocally declared that any form of privacy violation, such as unauthorised or unreasonable surveillance, must be eradicated.

Within the framework of unlawful surveillance targeting multiple journalists and members of the press, the Supreme Court, in the case of Anuradha Bhasin vs. Union of India [19], determined that journalists should be afforded the opportunity to engage in reporting activities. The court emphasised that there is no valid rationale for permitting a constant threat to loom over the press indefinitely, akin to the metaphorical sword of Damocles. The Supreme Court has saw regarding the state's authority to withhold certain information, stating that such action is permissible if it falls within the reasonable restrictions outlined in Article 19, clause 2. However, it is important to note that if the state attempts to infringe upon a citizen's fundamental rights, this cannot be tolerated. In such cases, it has been suggested that the Union of India should not adopt an adversarial stance when the fundamental rights of its citizens are at risk [20].

Based on the analysis of the aforementioned cases, it becomes apparent that the Supreme Court holds the view that illegal surveillance poses a clear and undeniable threat to the right to privacy. The court has consistently advised the government of India against infringing upon the fundamental rights of its citizens, unless such encroachment is deemed reasonable and bona fide in accordance with Article 19(2) of the

Constitution of India. Furthermore, the court has emphasised the importance of maintaining comprehensive records and logs of surveillance data in cases where surveillance is deemed a reasonable option. This measure is crucial in order to ensure that the fundamental rights of citizens are adequately protected.

VI. THE ADMISSIBILITY OF ILLEGALLY OBTAINED EVIDENCE: PRE PUTTASWAMY

The principle of evidentiary admissibility, which underpins the interpretation of evidence in India, is based on the principle of relevancy as outlined in Section 5 of the Evidence Act, 1872. The elucidation of the principle of relevancy can be further enhanced by consulting the delineation of a "relevant fact," as expounded in Section 2. According to the provisions of the Evidence Act, 1872, any fact is considered relevant to another fact if there is any kind of relationship or connection between the two. This means that if one fact has any bearing or significance on another fact, it is deemed relevant under the law. The provisions on admissibility under Indian law, specifically Sections 24 to 30, do not address the issue of illegality in obtaining evidence as a basis for exclusion. Therefore, it is unsurprising that the prevailing stance in Indian law has been established to prioritise the consideration of evidence, irrespective of its illegitimate acquisition [21-24].

The focal point of inquiry in the R.M. Malkani case pertained to the admissibility of a recorded conversation obtained via a tape-recording device affixed to the informant's telephone, as presented before the esteemed Supreme Court. According to the Supreme Court's ruling, it has been established that a particular piece of evidence may be deemed admissible, despite its illegal acquisition, unless the presiding judge exercises their discretionary power to deem such evidence inadmissible. This discretion is exercised when the evidence operates in an unfair manner against the accused party. Nevertheless, it is worth noting that in practice, the application of judgements based on the R.M. Malkani case has been infrequent, if not entirely absent, in providing the aforementioned advantage to the defendant. The Court made a regressive observation while investigating the violation of Article 21 of the Constitution and the right to privacy. It stated that the courts would not provide protection against wrongful or high-handed interference from the executive to individuals who are guilty of violating the law. Instead, such protection would only be extended to individuals who are innocent. This perspective of the Court implies a theoretical framework within the criminal justice system wherein the desired outcomes are considered more important than the methods employed to achieve them. Consequently, the attainment of a conviction or a committal is prioritised over concerns pertaining to individual liberties or privacy [25-27].

Regarding the case of Pooran Mal, it is noteworthy that the Supreme Court has once again reaffirmed the position that the admissibility of evidence in India can only be determined by applying the test of relevancy as prescribed in Section 5 of the Evidence Act, 1872. Therefore, the Court's perspective was that in cases where there is an allegation of a violation of fundamental rights, the admissibility of evidence obtained through an unlawful search cannot be disregarded. The position in question has consistently been upheld by the Supreme Court, as evidenced by its ruling in the Bharati Tamang case. Within the context of the Evidence Act, 1872, the lack of explicit guidance has resulted in the exercise of discretion through these judicial decisions. Consequently, individuals subjected to unlawful investigations have consistently found themselves in a position of disadvantage, as their rights have been compromised. Furthermore, it is evident that these judgements were made without taking into consideration the provisions outlined in Article 20(3) of the scheme. Under certain provisions, such as Section 5, individuals who are accused of wrongdoing may be subject to wiretapping without their awareness. This measure is justified on the basis that these individuals are perceived to pose a potential risk to national security or public order. The evidence acquired via the use of wiretapping techniques could subsequently be employed to implicate the aforementioned individual under investigation [28-31].

Regrettably, this aspect was not given due consideration. It is noteworthy to mention that the opinions expressed by R.M. Malkani and Pooran Mal were rendered subsequent to the ruling of the Supreme Court in the Kharak Singh case, wherein it was determined that the constitutional right to privacy is not explicitly protected under Article 21. The aforementioned judgements were rendered prior to the landmark Maneka Gandhi case 29, which introduced the notion of "due process of law" within the scope of Article 21. Therefore, it would be incorrect to rely on these judgements delivered prior to both the Kharak Singh case and the Maneka Gandhi case in order to claim that principles of policy and infringement of fundamental rights would not make illegally obtained evidence inadmissible. Therefore, in light of the K.S. Puttaswamy case, which acknowledged the right to privacy under Article 21, it is imperative that any evidence obtained through surveillance adheres not only to the criteria of the "procedure established by law" as outlined in Rule 419-A of the Telegraph Rules, 1951, or Section 5 of the Telegraph Act, 1885, but also satisfies the "due process"

examination established by the Puttaswamy case [32-38]. The present study demonstrates that any violation of a person's confidentiality by the state must satisfy three essential criteria:

- The presence of a legal framework or the legality of the measure implemented.
- The indispensability of the assessment performed in relation to a legitimate state objective.
- Proportionality, which guarantees a logical connection between the objectives pursued and the means employed to attain them.

VII. THE TELEGRAPH ACT AND PROCEDURAL SAFEGUARDS

The study conducted by Vinit Kumar and Jatinder Pal Singh aimed to investigate and analyse the judgements made in a particular context. The researchers sought to examine the factors influencing these judgements and their potential implications. Through their research, Kumar and Singh aimed to contribute to the existing body of knowledge in this field and shed light on the decision-making processes involved. According to Section 5(2) of the Telegraph Act, 1885, the Central Government, State Government, or any officer who has been granted specific authorization has the authority to intercept any message or messages sent to or received from any individual or group of individuals. This interception can take place during a public emergency or in order to ensure public safety. According to Rule 419-A(1) of the Telegraph Rules, 1951, in conjunction with Section 5(2), it is stipulated that any directive for interception can only be issued through an order issued by a secretary to the Government of India or by the Secretary to the State Government responsible for the Home Department. In exceptional circumstances, an officer of no lower rank than the Joint Secretary to the Government of India may issue such a directive.

Nevertheless, it is worth noting that Rule 419-A(1) does include a provision that allows for an exemption from the aforementioned requirement. Under certain circumstances, such as when it is not possible to obtain prior directions due to the location being in remote regions or due to operational constraints, an interception may be conducted with the prior authorization of the head or the second-most senior officer of the approved security and law enforcement division at the central level. Upon careful examination of Rule 419-A, it becomes apparent that the legislative framework has been designed in such a way as to limit the exercise of discretion exclusively to the executive branch. The hazards associated with the aforementioned subject matter are clearly discernible based on the rulings rendered by Vinit Kumar and Jatinder Pal Singh [39,40].

Regarding the Vinit Kumar case, the Central Bureau of Investigation (CBI) has put forth an allegation stating that the petitioner engaged in bribery with an official from a public sector bank in order to secure a credit-related favour. In order to carry out the necessary surveillance, three orders were issued under Rule 419-A with the purpose of intercepting the individual's telephone calls. The petitioner, in the present case, has raised a challenge against the three orders under scrutiny. The petitioner contends that the telephonic recordings, which were obtained unlawfully and are included in the charge sheet, as well as all the evidence gathered on its foundation, should be invalidated. In light of the recent Puttaswamy case, Ranjit More's judgement represents a significant departure from the traditional approach of disregarding privacy concerns when it comes to the admissibility of illegally obtained evidence. Instead, the judgement embraces the three-pronged test established in the Puttaswamy case, marking a notable shift in the treatment of this issue [41-44].

The analysis conducted in the judgement lacked a clear distinction between the evaluation of each of these prongs. Instead, the majority of the analysis was primarily focused on the first prong, which pertains to legality. As per the Court's observations, it was determined that, upon reviewing the available materials, there were no identifiable instances of "public safety" or "public emergency" in relation to the subject matter. Upon the absence of any material substantiating the aforementioned claims, the Court, in a comprehensive manner, invalidated the orders, asserting that the interception orders have not met the criteria of legality, necessity, and proportionality. Significantly, the Court further noted that endorsing a breach of fundamental rights based on the belief that in the criminal justice system, the desired outcomes validate any methods employed would constitute clear arbitrariness and disregard for the directives of the Supreme Court in the Puttaswamy case [45-48].

The Jatinder Pal Singh case involves allegations made by the Central Bureau of Investigation (CBI) regarding the petitioner's involvement in a criminal conspiracy with Dr. Ketan Desai, the President of the Medical Council of India. The alleged objective of this conspiracy was to secure recognition for courses offered by a medical college in violation of applicable rules and regulations. The revelation of this conspiracy occurred when the Central Bureau of Investigation (CBI) initiated the practice of conducting surveillance on mobile phones. The petitioner put forth the argument that the method used to subject the mobile phones to telephonic surveillance was deemed unlawful. Consequently, it was contended that no reliance could be placed on the evidence obtained through this means. Upon careful examination of the available records, it was

determined by the Court that there was a lack of sufficient evidence to support the notion that a thorough review of the Home Secretary's order had been carried out in accordance with Rule 419-A and the Telegraph Act. While the Court refrained from conducting a detailed examination of the Puttaswamy case due to the absence of any orders issued under Rule 419-A, unlike the Vinit Kumar case, it did assert that failure to comply with these Rules would result in evident arbitrariness and infringement of the fundamental rights of citizens. Consequently, the court has nullified the charges that were formulated against the petitioner [49-55].

VIII. SURVEILLANCE AND PRIVACY: POST PUTTASWAMY

The Indian government has implemented the Aadhaar Scheme, which involves the creation of a centralised biometric and demographic information database for its residents. The constitutionality of the Aadhaar Scheme was brought into question and subsequently challenged before the Supreme Court in 2012. During a hearing in 2015, the government asserted that, according to their interpretation, the Constitution did not establish a fundamental right to privacy. According to the Attorney General, there is a discrepancy between the Supreme Court's previous references to a right to privacy and its earlier rulings in MP Sharma v. Satish Chandra and Kharak Singh v. State of UP. While the Supreme Court has made some indications about the existence of a right to privacy in various cases, these statements seem to contradict the decisions made by the larger benches of the Supreme Court in the aforementioned cases. As a result, a panel of nine judges from the Supreme Court convened to deliberate on the question of whether the right to privacy was indeed recognised as a safeguarded privilege under the Indian Constitution in the case of Puttaswamy. Within this pivotal ruling, the Court reached a unanimous consensus that the right to privacy is an inherent component of the right to life and freedom of choice as outlined in Article 21. Furthermore, it is regarded as an integral aspect of the freedoms safeguarded by Part III of the Constitution [56,57].

The Supreme Court's ruling in this case effectively overturned the decisions made in the MP Sharma and Kharak Singh cases, which previously held that the right to privacy was not safeguarded by the Constitution. The significance of the striking down of these cases in Puttaswamy lies in its ability to provide insights into the evolution of the legal landscape concerning privacy and surveillance in India. Following the proceedings, a panel of five judges from the Supreme Court conducted a comprehensive evaluation of the Aadhaar scheme in relation to the right to privacy. The panel predominantly affirmed the constitutionality of the scheme, officially known as the Targeted Delivery of Financial and Other Subsidies, Benefits, and Services Act 2016, while simultaneously invalidating specific provisions. The number provided by the user is 19. The introduction of Puttaswamy and Aadhaar had a profound impact on the legal framework in India, manifesting itself in at least two discernible manners. Initially, the authors of the study explicitly acknowledged the negative consequences associated with surveillance, particularly in the context of the digital era. Furthermore, the authors of this study developed a hierarchical proportionality test that can be used in the context of a legal dispute involving fundamental rights [58-60].

IX. THREAT TO PRIVACY DUE TO SURVEILLANCE

The presence of a state surveillance apparatus, irrespective of its practical utilisation, has a direct impact on individual liberty and the ability to exercise freedom of speech and expression. Privacy, beyond being a mere negative right of non-interference, plays a crucial role in fostering human intimacy and facilitating the free expression of unpopular or unconventional ideas, shielded from social disapproval or adverse outcomes. Similarly, a digital surveillance system resembling the Panopticon hinders freedom of expression and openness simply due to the individual's awareness of being under constant observation. Subba Rao J., in his dissenting opinion in the Kharak Singh case, provided a comprehensive explanation regarding the impact of surveillance on individuals. He highlighted that surveillance imposes psychological restraints, which subsequently influence freedom of thought and expression, ultimately affecting personal liberty. During the case of Puttaswamy, the nine-judge bench acknowledged the constitutional correctness of Subba Rao J's dissent while overturning the decision made in Kharak Singh [61-64].

Subba Rao J demonstrated remarkable foresight, as contemporary governments possess the capability to intercept our confidential dialogues, scrutinize our private correspondences, and meticulously monitor our daily whereabouts. When people know that the government might monitor their communications and movements, they may be less inclined to exchange radical ideas or participate in political gatherings. This apprehension stems from a fear of potential repercussions for expressing dissenting opinions. An alternative perspective argues that surveillance significantly impacts the fundamental right to privacy, especially when it comes to intellectual privacy. This concept encompasses the essential liberty to cultivate and nurture ideas

without the encumbrance of constant monitoring. Additionally, surveillance also has implications for informational privacy, a multifaceted concept that encompasses notions of secrecy, control, and anonymity. The apprehension regarding the potential disclosure of private details pertaining to an individual's way of life and personal decisions has been observed to have a verifiable impact on freedom of expression and association. This impact manifests in the form of inhibiting or dissuading individuals from engaging in the consumption and exchange of unconventional, unpopular, controversial, or offensive concepts. 2017 marked a significant milestone in the incorporation of these ideas into India's constitutional articulation of privacy, as explicitly stated in the Puttaswamy judgment [65-70].

Puttaswamy's contribution to the field of Indian court proceedings was significant as it broadened the range of terminology that could be used when addressing surveillance-related cases. Puttaswamy enhanced the understanding and discourse surrounding this subject matter within the legal system by providing a more detailed explanation of the significance of privacy and its perceived infringement in surveillance instances. Considering the inherent power asymmetry between the general populace and the governing body, it is reasonable to anticipate a greater degree of privacy protection when it comes to individuals vis-à-vis the state, in contrast to interactions involving private citizens. The observed phenomenon can be attributed to the centralization of authority within the state, which results in the state's exclusive control over the use of force and the potential for its improper utilisation. The absence of a statutory framework and limited accountability surrounding various law enforcement agencies, such as the Central Bureau of Investigation (CBI), the Intelligence Bureau (IB), and the Research & Analysis Wing (R&AW), particularly accentuate the aforementioned concerns within the context of India. Within the given context, the implementation of surveillance serves to amplify the existing power imbalance between the state and its citizens. As Richards highlighted, this asymmetry can lead to the selective application of laws, instances of discrimination, and the exploitation of individuals through blackmail. This particular scenario further heightens the risks associated with secret surveillance. Through the recognition of the psychological limitations resulting from surveillance, as exemplified in the dissenting opinion in the Kharak Singh case, Puttaswamy implicitly acknowledges the inherent risks associated with the covert nature of state surveillance. This covert practice robs individuals of their ability to determine whether they are under surveillance [71-74].

Researchers have found that the fear of potential government surveillance significantly influences individual behavior, potentially reducing the capacity for "critical subjectivity." This concept, crucial to the functioning of a democratic society, refers to the ability of individuals to engage in independent and critical thinking. The intensification of privacy harms caused by surveillance is particularly pronounced in the era of advanced technology. The advent of technology has greatly facilitated and bolstered the state's capacity for comprehensive GPS monitoring, data mining, and profiling. Furthermore, it has streamlined the process of collecting and analysing metadata, thereby enabling more efficient and effective surveillance practices. The augmentation of the state's ability to intrude upon the realm of personal privacy has resulted in an uneven distribution of power between the populace and the governing body. This consolidation of authority poses a significant threat to the principles of a constitutional democracy [75,76]. In his concurring opinion in the Puttaswamy case, Kaul J. astutely recognised the inherent risks that technology presents to the concept of privacy. He aptly noted that “The growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance in ways that are unimaginable.”

This observation aligns with the positions held by various other legal systems. Within the United States, it is worth noting that the concurring opinions expressed in the case of US v. Jones recognised the fact that in the era prior to the advent of computers, the most significant safeguards for privacy were not derived from constitutional or statutory provisions but rather from practical considerations. The aforementioned reasons for the adoption of alternative surveillance methods stem from the inherent limitations of traditional surveillance techniques. These conventional methods necessitated significant investments of both time and financial resources, making them impractical for widespread implementation. Additionally, the scalability of traditional surveillance methods was severely restricted, posing challenges to effectively monitoring larger areas or populations. Moreover, the reliance on limited police resources further compounded the inefficiencies of traditional surveillance approaches. Contemporary surveillance techniques, conversely, exhibit a greater capacity for information acquisition, particularly when surveillance is conducted over an extended period of time. The aforementioned harms recognise the societal benefit that the entitlement to privacy provides, its significance within a constitutional democracy, and its role in protecting the rights of marginalised individuals. When examining the constitutionality of illegally obtained evidence and the absence of judicial oversight over surveillance actions, it is crucial to recognise the significant role that they will play [77-80].

X. THE STANDARD FOR TESTING PRIVACY VIOLATIONS

The recognition by Indian courts regarding the constitutionality of a government measure that restricts rights emphasises the importance of striking a proper balance between fundamental rights and state action that imposes limitations on these rights. Achieving this equilibrium necessitates considering the "disproportion of the imposition" and considering both the essence of the entitlement and the objective of the limitation. It is worth noting that the Indian courts seemed to have overlooked this aspect, as can be observed from the ruling in the case of Maneka Gandhi v. Union of India [81-83].

It was Maneka Gandhi who introduced the concept that the rights safeguarded by the Indian Constitution are not isolated from one another but rather interconnected. She argued that we should evaluate any law that restricts personal freedom (as stated in Article 21) in light of the principle of equality (as stated in Article 14). This evaluation is necessary to ensure that such a law is fair, just, and reasonable in substance. Nevertheless, the decision exhibited a degree of ambiguity regarding its precise implications. We learned that a law restricting freedom must not be arbitrary, fanciful, or oppressive to be considered reasonable. We set the aforementioned criterion at a relatively modest level, which allows for meeting it by demonstrating a valid governmental aim, as any capricious action would imply a complete lack of rationality. Nevertheless, it is noteworthy that the concept of proportionality in Indian constitutional jurisprudence has experienced a resurgence, thereby providing further substance to the notion that a law should possess qualities of fairness, justice, and reasonableness. Puttaswamy and Aadhaar's cases have made significant contributions to the development of proportionality analysis. However, some scholars argue that these cases missed the opportunity to establish a more precise and rigorous test. Nevertheless, these two cases have provided valuable insights into the criteria that a law must satisfy in order to be considered fair, just, and reasonable. The Puttaswamy plurality asserts that the procedural and content-based mandate of Article 21 requires the fulfilment of certain criteria to evaluate privacy restrictions [84-87].

The concept of legality in Indian constitutional jurisprudence underscores the fundamental principle that any encroachment on fundamental rights must be supported by legislative measures. Four key elements comprise the proportionality test: legitimacy, suitability, necessity, and balancing. These elements work together to assess the proportionality of a particular action or decision. Legitimacy refers to the requirement that the action or decision be based on a legitimate objective or purpose. Suitability examines whether the means chosen to achieve the objective are appropriate and effective. The necessity test determines whether the action or decision is the least restrictive or intrusive option available. Finally, balancing involves weighing. The precise doctrinal origin of procedural safeguards remains uncertain. However, a careful examination of judgements delivered by the European Court of Human Rights (ECtHR) suggests that the necessity for these safeguards may potentially be attributed to a positive duty imposed on the state to protect confidential data, even in cases where a measure impinging on privacy enables governmental access to such private information. The schema mentioned earlier underwent a revision in the context of Aadhaar. There has been considerable debate surrounding the necessity component of the proportionality test, specifically regarding the relevance of the 'least intrusive' criterion. In the majority opinion, Sikri J. expounded on the proportionality standard, which consists of four distinct components [87-90].

According to the established framework, the implementation of a rights-restricting measure must adhere to several key stages. First and foremost, the measure must have a legitimate objective or appropriate purpose, ensuring that it serves a valid objective. Secondly, the measure must be a suitable means of advancing this goal, demonstrating a rational connection between it and its intended purpose. Thirdly, it is crucial to consider whether there exist any alternative approaches that are equally effective in achieving the desired outcome while being less restrictive. This necessity stage requires a thorough exploration of potential alternatives. Lastly, the measure must not disproportionately affect the right holder, requiring a careful balance between the necessity of achieving the aim and the limitations placed on the right. It is imperative to establish a proper relationship between these factors to ensure a fair and just implementation of the measure. The aforementioned statement seems to align with the principles of Legitimacy, Suitability, Necessity, and Balancing as outlined in the Puttaswamy case. It has been pointed out, though, that Aadhaar chose a less strict approach based on the research of Professor David Bilchitz instead of a stricter one where the government would have had to show that there wasn't a less strict but equally effective alternative to meet the necessity requirement of the proportionality test [91-93].

XI. JUDICIAL OVERSIGHT OVER SURVEILLANCE: AN EXAMINATION OF ITS CONSTITUTIONAL NECESSITY DURING POST-PUTTASWAMY

Although Puttaswamy and Aadhaar do not explicitly address India's surveillance infrastructure's constitutionality, they provide valuable insights into the potential negative consequences of surveillance and emphasize the importance of judicial supervision in this context. As a preliminary consideration, it is imperative to comprehend the underlying rationale for the desirability of judicial oversight within a legal system that upholds the principle of the rule of law. The Indian Supreme Court has determined that Article 14 of the Constitution, which guarantees equality before the law, constitutes a component of the rule of law. This principle necessitates the resolution of fundamental rights through a separate and impartial judicial body [93-94].

One of the reasons for the importance of having impartial judges is the need to resolve disputes regarding the legality of governmental action. It is crucial that these judges are independent from the executive branch in order to ensure fairness and objectivity in the decision-making process. The absence of accountability, specifically in the context of judicial scrutiny, poses a significant threat to the rule of law. Furthermore, it disrupts the balance of power between the executive and judiciary, specifically in terms of horizontal separation of powers. The necessity for inter-branch oversight, particularly in the realm of judicial oversight, concerning intrusive state action arises from the fundamental principle of the rule of law. The concept under discussion extends beyond the boundaries of India. The European Court of Human Rights (ECtHR) emphasised in the case of Klass v. Germany that although courts are not obligated to replace the policy evaluation of the legislature, it is important to note that while the threat of terrorism is indeed a legitimate concern, states are not granted unrestricted authority to subject individuals within their jurisdiction to covert surveillance. One of the key principles of the rule of law is that any infringement on an individual's rights by the executive branch should be subject to effective oversight. The judiciary typically provides this oversight, offering the highest level of independence, impartiality, and adherence to proper procedures. The dilution of the rule of law resulting from a lack of judicial oversight has significant consequences, particularly for individuals. Therefore, it becomes necessary to examine the effects on individual rights through rigorous testing and analysis [93-96].

i. The Governing Statutory Framework

As previously indicated, the regulatory framework for surveillance in India is governed by Section 5(2) of the Telegraph Act 1885 and Section 69 of the Information Technology Act 2000 (IT Act 2000), along with the corresponding rules established under these statutes [97]. Typically, in both regimes, the responsibility for authorising the interception, monitoring, and decryption of communication lies with the Secretary to the Government of India in the Ministry of Home Affairs at the national level and with the Home Secretary at the state level. The existing framework lacks provisions for pre-authorization judicial oversight of surveillance activities conducted by the executive branch. Specifically, view stage, the authority to assess the compliance of directions issued by the authorising agency with the statute is solely entrusted to the executive branch, specifically through a review committee. The composition of the Review Committee at the Centre includes the Cabinet Secretary, the Secretary to the Government of India, Legal Affairs, and the Secretary to the Government of India, Ministry of Telecommunications. The Review Committee's decision is final and immune to parliamentary or judicial scrutiny. Furthermore, it is worth noting that there is no stipulation mandating the provision of a hearing to the individual under surveillance at any point in the process. In 1997, a significant challenge to the surveillance framework emerged with the case of PUCL, which raised concerns about the constitutionality of Section 5(2) of the Telegraph Act. The assertion was made that the implementation of a pre-existing judicial examination of a telephone interception directive was the sole method to ensure the protection of privacy rights. Nevertheless, it is worth mentioning that there is no specific legal requirement for judicial oversight in this matter. Instead, the Supreme Court based its decision on the existing English law outlined in the Interception of Communications Act of 1985. The court concluded that incorporating prior judicial scrutiny as a procedural safeguard was not feasible. The court upheld the constitutionality of the Telegraph Act and issued a set of guidelines. These guidelines ultimately resulted in Rule 419A being included in the Telegraph Rules. We implemented the aforementioned guidelines as protective measures to prevent the misuse of surveillance powers [97-100].

ii. Judicial Oversight: An Essential Component of the Constitutional Framework

According to the available evidence, surveillance has a significant impact on the fundamental right to privacy, which is inherent in Article 21 of the Constitution. One important consideration is whether the current surveillance framework, without any involvement or supervision from the judiciary, would meet the required standard for evaluating privacy infringements. The authorization of surveillance is supported by legal

frameworks, specifically the Telegraph Act of 1885 and the IT Act of 2000. Thus, given that the condition of legality is fulfilled, our analysis will focus solely on evaluating whether the lack of independent judicial oversight undermines the various stages of the proportionality test and whether this system includes sufficient safeguards to prevent abuse [101].

XII. CONCLUSION

Our research has determined that the Puttaswamy case does not fall under the category of surveillance. However, India's contribution lies in its intricate web of concepts that elucidate the various facets of privacy, addressing the ramifications of surveillance directly. In conjunction with Aadhaar, the framework serves as a means to evaluate the effectiveness of the current legal system that regulates surveillance activities. The current legal framework in India enables the state to disregard individual liberties without facing consequences. The absence of both ex ante and ex post judicial oversight in granting exclusive executive control over secret surveillance raises concerns regarding the denial of due process. When surveillance activities lead to a legal trial, the courts become implicated in the violations that occurred during the unconstitutional surveillance. The courts admit the evidence from such surveillance, following the default admissibility rule. The government's provision of unlimited discretion in the realm of surveillance raises concerns about its potential impact on democratic principles. Some argue that this provision could potentially undermine or even dismantle democracy in the name of its protection. Building on the famous Puttaswamy case, which showed how important privacy is for protecting people's freedom, our research aims to show that the groundwork has been laid for supporting judicial oversight and putting in place a rule that doesn't allow evidence that was obtained by violating privacy rights to be used in court. These cases provide an opportunity to redirect our attention towards the liberty perspective. This is because rights, at their core, suggest that the state is obligated to provide a justification for every intrusion, even if it comes at the expense of efficiency.

It is clear that additional statutes are needed to impose more rational limitations on unauthorized monitoring and data gathering. It is evident that there is currently a lack of regulatory framework in place to safeguard data and monitor the unauthorised acquisition and storage of both personal and non-personal information belonging to individuals. Across different countries, there are diverse laws that grant governments the authority to retain individuals' data. For instance, in Russia, such legislation can potentially lead to reduced transparency and heightened infringement upon individuals' legal rights. Therefore, it is imperative to implement more expansive and all-encompassing legislation in our nation, considering the substantial population of India and the escalating number of individuals engaging in digital activities. It is incumbent upon the government to guarantee the populace that their shared data remains safeguarded and impervious to unauthorised access by any external entities.

XIII. ACKNOWLEDGMENT

The authors acknowledge the Department of Amity Law School for critically reviewing the manuscript and providing the feedbacks.

REFERENCES

[1]. Zachary Smith, 'Privacy and Security Post Snowden: Surveillance Law and Policy in the United States and India' (2014) 9 Intercultural Human Rights Law Review 137, 192-95, 197; Ronald Krotoszynski Jr, Privacy Revisited (OUP 2016) 169-71, 181-82, 186.

[2]. Robyn Greene, '*How the Government Can Read Your Email*' (Politico, 22 June 2017).

[3]. 'Secret Operating Procedure for Digital Snooping Revealed. Confirms Fears of Centralisation of Executive Power, Zero Judicial Scrutiny and Oversight' (Internet Freedom Foundation, 11 March 2019).

[4]. Sarah Brayne, 'Big Data Surveillance: The Case of Policing' (2017) 82(5) American Sociological Review 977, 979.

[5]. Chaitanya Ramachandran, '*PUCL v. Union of India Revisited*: Why India's Surveillance Law Must Be Revised for the Digital Age' (2014) 7 National University of Juridical Sciences Law Review 105, 112-14, 117; Vipul Kharbanda, 'Policy Paper on Surveillance in India' (The Centre for Internet & Society, 3 August 2015).

[6]. State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600 [154]-[155]; Umesh Kumar v State of Andhra Pradesh (2013) 10 SCC 591 [35]. See Talha Rahman, 'Fruits of the Poisoned Tree: Should illegally obtained evidence be admissible?' (2011) Practical Lawyer April S-38

[7]. (2017) 10 SCC 1.

[8]. (2019) 1 SCC 1.
[9]. *PUCL v Union of India* (1997) 1 SCC 301 [17];Dnyaneshwar v State of Maharashtra (2019) SCC Online Bom 4949 [18].
[10]. PRS Legislative Research. 2021. The Personal Data Protection Bill, 2019.
[11]. Thelawreviews.co.uk. 2021. The Law Reviews - The Privacy, Data Protection and Cybersecurity Law Review. [online].
[12]. Sharma, D., Sharma, D. and Sharma, D., 2021. Australia | New surveillance law allows government to quietly modify your social media posts in Australia | SCC Blog.
[13]. The Indian Express. 2021. Explained: The laws for surveillance in India, and concerns over privacy.
[14]. Telegraph Act, 1885.
[15]. Telegraph Act, 1885, S. 5.
[16]. PUCL vs. Union of India MANU/SC/0149/1997
[17]. Manohar Lal Sharma vs. UOI and Ors. MANU/SC/0989/2021
[18]. K.S Puttaswamy v. Union Of India MANU/SC/1044/2017
[19]. Anuradha Bhasin v. Union of India MANU/SC/0022/2020
[20]. Ram Jethmalani v. Union of India MANU/SC/0711/2011
[21]. Evidence Act, 1872, S. 5.
[22]. Evidence Act, 1872, S. 2.
[23]. Evidence Act, 1872, Ss. 24, 25, 26, 27, 28, 29 and 30.
[24]. Law Commission of India, Report No. 94, Evidence Obtained Illegally or Improperly: Proposed Section 166-A, Indian Evidence Act, 1872, (October 1983), Para 3.1. For example, in Sunder Singh v. State of U.P. AIR 1956 SC 411, para 9, the judgment referred to by the Commission to put forth its case, the irregularity in the search and recovery procedure did only at the highest effect the "weight" of the evidence.
[25]. R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471.
[26]. R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471, para 24.
[27]. R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471, para 24.
[28]. Pooran Mal v. Director of Inspection (Investigation), (1974) 1 SCC 345.
[29]. Evidence Act, 1872. 23. Pooran Mal v. Director of Inspection (Investigation), (1974) 1 SCC 345, para 23.
[30]. Bharati Tamang v. Union of India, (2013) 15 SCC 578, para 28.
[31]. Constitution of India, Art. 20(3).
[32]. (1973) 1 SCC 471. 27. (1974) 1 SCC 345.
[33]. Kharak Singh v. State of U.P., AIR 1963 SC 1295.
[34]. Maneka Gandhi v. Union of India, (1978) 1 SCC 248, para 48.
[35]. AIR 1963 SC 1295.
[36]. (1978) 1 SCC 248.
[37]. (2017) 10 SCC 1, para 652.2.
[38]. (2017) 10 SCC 1.
[39]. 2019 SCC OnLine Bom 3155.
[40]. 2022 SCC OnLine Del 135.
[41]. 2019 SCC OnLine Bom 3155.
[42]. Vinit Kumar case, 2019 SCC OnLine Bom 3155, para 2.
[43]. (2017) 10 SCC 1.
[44]. (2017) 10 SCC 1.
[45]. Vinit Kumar case, 2019 SCC OnLine Bom 3155, para 19.
[46]. Vinit Kumar case, 2019 SCC OnLine Bom 3155, para 20.
[47]. (2017) 10 SCC 1.
[48]. Vinit Kumar case, 2019 SCC OnLine Bom 3155, para 42.
[49]. 2022 SCC OnLine Del 135.
[50]. Jatinder case, 2022 SCC OnLine Del 135, paras 2(i) and (ii).
[51]. Jatinder case, 2022 SCC OnLine Del 135, para 6(b).
[52]. Jatinder case, 2022 SCC OnLine Del 135, para 57.
[53]. (2017) 10 SCC 1.
[54]. 2019 SCC OnLine Bom 3155.
[55]. Jatinder case, 2022 SCC OnLine Del 135, para 59.

[56]. PUCL v Union of India (1997) 1 SCC 301 [17];Dnyaneshwar v State of Maharashtra (2019) SCC Online Bom 4949 [18]
[57]. Puttaswamy (n 10) [4]-[6].
[58]. Gobind v State of MP (1975) 2 SCC 148; R Rajagopal v State of TN (1994) 6 SCC 632; PUCL (n 12).
[59]. (1954) SCR 1077.
[60]. (1964) 1 SCR 332.
[61]. Article 21 of Constitution of India 1950.
[62]. Article 14 of Constitution of India 1950.
[63]. Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 193-95.
[64]. Charles Fried, 'Privacy' (1968) 77 Yale Law Journal 475
[65]. Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 Mississippi Law Journal 213, 240-51.
[66]. Kharak Singh (n 16).
[67]. Puttaswamy (n 10) [17] [22] [24] (Chandrachud J), [341]-[344] (Chelameswar J), [446] [452] [475] (Nariman J); Aadhaar (n 11) [168].
[68]. Neil Richards, 'Intellectual Privacy' (2008) 87 Texas Law Review 387, 389.
[69]. R v Spencer (2014) 2 SCR 212 [38]-[47] (Canadian Supreme Court).
[70]. Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) 93(2) Journalism & Mass Communications Quarterly 296; Alex Mathews and Catherine Tucker, 'Government Surveillance and Internet Search Behavior' (2017).
[71]. Laurent Sacharoff, 'The Relational Nature of Privacy' (2012) 16(4) Lewis & Clark Law Review 1249, 1282-83; Neil Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1955.
[72]. Committee of Experts under the Chairmanship of Justice BN Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018) 123.
[73]. Richards, 'Dangers of Surveillance' (n 33) 1935, 1957.
[74]. Daniel Solove, 'I've Got Nothing to Hide' (2007) 44 San Diego Law Review 745, 758; Julie Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904, 1912; Richard Clarke et al, 'Liberty and Security in the Changing World' (2013) White House Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies 47.
[75]. Christina Moniodis, 'Moving from Nixon to NASA: Privacy's Second Strand - A Right to Informational Privacy' (2012) 15(1) Yale Journal of Law and Technology 139, 154; Puttaswamy (n 10) [304].
[76]. Kyllo v United States 533 US 27, 34 (2001) (US Supreme Court); Carpenter v United States No 16-402, 138 S Ct 2206 (2018) 6 (US Supreme Court).
[77]. Puttaswamy (n 10) [585].
[78]. 565 US 400 (2012) (Sotomayor J and Alito J concurring) (US Supreme Court).
[79]. Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89 Yale Law Journal 421, 455; Chinmayi Arun, 'Paper-Thin Safeguards and Mass Surveillance in India' (2014) 26 National Law School India Rev 104, 114; Kirsty Hughes, 'Mass Surveillance and The European Court of Human Rights' (2018) 6 European Human Rights Law Review 589, 598.
[80]. David Gray and Danielle Citron, 'The Right to Quantitative Privacy' (2013) Minnesota Law Review 62, 79
[81]. Chintaman Rao v State of MP (1950) SCR 759, 763.
[82]. State of Madras v VG Row (1952) SCR 597, 607.
[83]. (1978) 2 SCR 621, 667-73.
[84]. Tarunabh Khaitan, 'Beyond Reasonableness – A Rigorous Standard of Review for Article 15 Infringement' (2008) 50(2) Journal of Indian Law Institute 177, 191.
[85]. Om Kumar v Union of India (2001) 2 SCC 386; Teri Oat Estates v UT Chandigarh (2004) 2 SCC 130; Modern Dental College & Research Centre v State of MP (2016) 7 SCC 353.
[86]. Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere?' (2020) 3(2) U of OxHRH J 55.
[87]. Puttaswamy (n 10) [310] (Chandrachud J).

[88]. See State of Madhya Pradesh v Thakur Bharat Singh [1967] 2 SCR 454; Bishan Das v State of Punjab [1962] 2 SCR 69.

[89]. Craxi (No 2) v Italy (2003) ECHR 25337/94 [73], [74] (European Court of Human Rights).

[90]. The State argued that the least intrusive standard was not a part of proportionality, whereas the Petitioners argued that such a standard ensured a minimal invasion of privacy. See Aadhaar (n 11) [292] (Sikri J), [816] (Bhushan J), [1261] (Chandrachud J).

[91]. Mariyam Kamil, 'The Aadhaar Judgment and the Constitution – II: On Proportionality' (Indian Constitutional Law and Philosophy, 1 September 2017)

[92]. Aadhaar (n 11) [158] (Sikri J).

[93]. Aparna Chandra, 'Privacy and Women's Rights' (2017) 52(51) Economic and Political Weekly 46, 48.

[94]. Union of India v Madras Bar Association (2010) 11 SCC 1 [101] [102].

[95]. Ann Cavoukian, 'Privacy, Transparency, and the Rule of Law: Critical to Preserving Freedom and Liberty' (2005) 19 National Journal of Constitutional Law 193, 196; Hughes (n 44) 592-93, 596.

[96]. (1979-80) 2 EHRR 214 (European Court of Human Rights).

[97]. Indian Telegraph Rules 1951, Rule 419A(1)-(2); The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, Rule 2(d) read with Rule 2(3).

[98]. Indian Telegraph Rules 1951, Rule 419A(16) and (17); IT Rules 2009, Rules 2(q) read with Rule 7 and Rule 22.

[99]. (1997) 1 SCC 301.

[100]. Ramachandran (n 4) 111-12.

[101]. Srikrishna Report (n 34) 125-126.