

Between Security and Liberty, A Critical Study of India's Evolving Digital Surveillance Framework

Urvashi Solanki¹, Salori Solanki²

^{1,2}*School of law, Devi Ahilya Vishwavidyalaya Indore*

Abstract—In the modern era of advanced technology, have transformed modes of living which were labour intensive, time consuming and produced limited outcomes. Digital systems now offer faster more efficient and effective results with minimal human efforts. This Increase reliance on technology has reshaped governance, communication and daily functioning. Some individuals exploit digital technologies for personal gain, which increase the State's responsibility to address cybercrimes and to protect the national security. The administrative agencies use this digital surveillance in the investigation procedure that helps them in various ways to reach out to the offenders digitally. Executive authorities trace the locations and activities of the fugitive offenders as a preventive Action against the offenders. Techniques are such as phone tapping, face identification, AI based and Biometric identification have become integral to modern investigative and preventive frameworks. Moreover, the increasing reliance on these techniques creates a fundamental tension between administrative law which guides the executive in protecting national security and penalizing cybercrimes and the Indian Constitution which guarantees the right to life and personal liberty under Article 21. To balance these competing interests, the court examines the extent to which the state may invade upon individual privacy for national security purposes ensuring that executive actions are not arbitrary or disproportionate the court applies the doctrines of proportionality and the doctrine of necessity to balance individual right with state authority.

This study highlights the ongoing conflict between digital privacy as a fundamental right and state actions examining the constitutionality of digital surveillance and the applicable legal framework in India. The study adopts a doctrinal approach analysing constitutional provisions, statutory analysis, and judicial precedent. It

is Observe that national security concerns may under due process limits fundamental rights which are not absolute.

Index Terms—Digital Surveillance, National Security, Administrative law, Right to Privacy, Constitutional Law, Doctrine of Proportionality, Doctrine of Necessity.

I. INTRODUCTION

In contemporary world, almost every activity performed by individuals such as using a smartphone, browsing the internet, paying a bill, sharing a photo, etc. creates a series of information and leaves the digital footprint behind it.¹ These digital era had transformed everyday life making communication, work and governance more efficient.² As the same, they have raised a question regarding to this matter is how much the state can monitor activities by which it becomes more important. As technology grows faster than regulation of laws, it means the need to examine the legal aspects and constitutional boundaries becomes urgent and unavoidable. Digital Surveillance is one of the most debated issues in this time between promise of safety and fear of overreach.

With the growth of Internet, they also have new challenges like cybercrimes such as identity theft, fraud, harassment, data breaches and cyber terrorism have increased rapidly which affecting the anonymity provides by digital space. Issue arises which makes complications in digital field is Weak International cooperation, jurisdictional barriers and deficiency of trained cyber experts. In response to these activities, governments of all countries including India relied

¹ S Srikumar, 'Digital Traces and Data Rights in India' (2024) 12(2) NALSAR Law Review 77

² Ministry of Electronics and Information Technology, Digital India Programme: Annual Report 2023–24 (Government of India 2024).

strongly on digital surveillance. Tools such as facial recognition, CCTV networks, biometric databases, mobile interception devices and social media monitoring become centric to national security and law enforcement strategies. These technologies help to prevent crimes and safeguard public order which has also risks of illegal activities and misuse and excessive state power. These ensures that surveillance does not weakens the personal liberty or turn into unchecked operations is a major constitutional challenge.

Digital surveillance refers to the procedure of collecting, operating and analysing electronic communication and digital tools. Authorities or organizations that deal with the issue of using surveillance to facilitate government control and maintain public order, track criminal activities and protect national security. In other words, Surveillance denotes the continuous observation of person, communication or surroundings by State agencies. It serves as an instrument to prevent offences, gather intelligence and respond to threat, Modern governance, involves various forms of digital & Physical surveillance, Including monitoring & e-mail, telephone Calls & CCTV footage.³

To protect the individual's rights several laws have been enacted by the Parliament including the Constitution of India 1950, which provides fundamental rights such as Article 21, the right to life and personal liberty, which recognizes the right to privacy,⁴ and Article 19(2), the freedom of speech and expression, which protects citizen's rights against surveillance, Indian Telegraph Act,1885 provides deception, interception and disclosure of any message under during an emergency for public safety or for the sovereignty and integrity of India or for the prevention of incitement or commission of an offence.⁵

The Information Technology Act, 2000, provides protection against cybercrimes and it is the primary law governing digital surveillance and data privacy It includes certain sections, such as Section 69 (Power to issue directions for interception and monitoring) , Section 69 A (blocking public access to information) ,

Section 69 B (monitoring of information traffic for cyber security) and Section 80 (powers of police officers and authorised officers to enter, search and arrest)⁶. The Criminal Procedure Code, 1973 or the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 provides procedures for criminal investigation of digital surveillance or data collection.⁷ The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,2016 also known as the Aadhaar Card Act 2016, provides biometric authentication, financial records, medical records and education purposes. It stores information or data of a single person in the form of an Aadhaar card⁸. Overall, these laws give the government the power to make rules and regulations regarding data surveillance and the protection of national security and individual privacy.

The legal challenge majorly affects digital surveillance as there is no proper enactment that safeguard personal privacy. In this regard, the Supreme Court recognized privacy as a fundamental right in the landmark judgement K.S. Puttaswamy (Retd.) V. Union of India⁹, surveillance is important for data protection.

To maintain balance between the harmony in the state autonomy and individual rights, the courts apply the principle of Proportionality, this principle explains that any restriction impose by state on fundamental rights must be justified, necessary and equitable to achieve the desired goal. Courts rely on proportionality doctrine to check surveillance actions of the states are limited to avoid misuse of discretionary power results in arbitrary results.

Digital surveillance is not only a national concern but also a global concern, therefore a global framework for digital surveillance and privacy are enacted which includes UN guidelines for the regulation of computerised personal data files,1990 gives the principles of fairness, transparency and accountability in data protection and the European Union's General Data Protection Regulation (GDPR), 2018 has globally worked for all data protection and regulation of data processing.

³ Dr Rumi Dhar and Sonia Nath, 'Digital Surveillance and Civil Rights: Assessing the Impact on Privacy' (2024) 5(1) Chanakya Law Review 66.

⁴ K.S. Puttaswamy (Retd.) V. Union of India (2017) 10 SCC 1

⁵ Indian Telegraph Act, 1885, Section 5(2)

⁶ Information Technology Act, 2000 Section 69, 69A, 69B, 80

⁷ Criminal Procedure Code, 1973 and Bhartiya Nyaya Suraksha Sanhita, 2023

⁸ Aadhaar Act, 2016

⁹ Ibid 4

In summary, the Internet is an essential tool of human life and it has both negative and positive impacts. However, with the rise of technological advancement the Internet has moved towards cyber-crimes and for the protection of individual's security and privacy, there is a need for digital surveillance and for that, there is a need for proper law. Therefore, this study aims to analyse digital surveillance, its challenges, evolution and scope in India and how the country can reach a proper method to deal with it in the modern era.

II. HISTORICAL BACKGROUND

The concept of Surveillance in India emerged during the colonial era, where it gradually evolved from localised Intelligence mechanism into a more structured administrative intelligence laws primarily aimed to regulate and control Indians. During this period the Britishers were relied extensively on surveillance not only to maintain law and order but also to scrutinize political dissent or mobilisation against the colonial rule¹⁰.

The revolutionary step taken by. The Indian revolutionaries in 1857 raised the concerns of British government for the urgent need of centralised and administrative intelligence structure capable of detecting conspiracies, monitoring communications. Further, the British government commence with the surveillance practices through formal legal mechanisms. The primary legislation passed by the British Parliament was the Police Act of 1861 which established the structure and hierarchy of the police force primarily answerable to the colonial

administrators¹¹ that time the surveillance measures were only for the prevention of crime, but also concerned with the maintaining the political stability and detecting nationalist movement against the country. Additionally, several laws like Indian Penal Code, Criminal Procedure Code, the Indian Telegraph Act, 1885 was enacted entrusted the government with exclusive power to intercept telegraphic communication on grounds of public safety and national security¹². Similarly, the Post Office act which permitted authorities to open and examine letters, while the Criminal Tribes Act 1871, which categories communities as hereditary criminals, subjected to strict surveillance, mandatory registration, and restricted movement which shows that how surveillance was used as a tool as social control and collective punishment rather than individual.

During World War II, some emergency laws were enacted such as Defence of India Acts 1951 Royal Act 1990 result in expansion of authority power for the preventive detention, communication and widespread monitoring of public activities.¹³ To tackle these operations some specialised agencies and authorities were setup, such as Intelligence Bureau 1809, Criminal Investigation Department which monitors the actions and activities of nationalist leaders to suppress the freedom struggle.¹⁴ Some surveillance measures used by the agencies were use of informants, Postal Interception, Telegraph monitoring.¹⁵ Through these measures of British regime gave India a formulated structure aimed at consolidating colonial power by restricting political freedoms, public order and most importantly to protect the national security.¹⁶

¹⁰ Apar Gupta, Digital Surveillance and Privacy in India: Legal and Ethical Dimensions (2021) 16 Indian Journal of Law & Technology <https://vidhilegalpolicy.in/wp-content/uploads/2021/06/IJLT-Vol-161.pdf> accessed 2 December 2025.

¹¹ Apar Gupta, Digital Surveillance and Privacy in India: Legal and Ethical Dimensions (2021) 16 Indian Journal of Law & Technology <https://vidhilegalpolicy.in/wp-content/uploads/2021/06/IJLT-Vol-161.pdf> accessed 2 December 2025.

¹² D Prasannakumar, 'Reassessing the Indian Telegraph Act 1885 in the Light of the Right to Privacy' (2025) Social Science Research Journal

<https://www.socialsciencejournals.net/archives/2025/vol7issue2/PartA/7-2-12-435.pdf> accessed 2 December 2025.

¹³ Ujjwal Kumar Singh, 'Surveillance, Public Order and Colonial Governance in India' (2007) International Review of Sociology 17(3) 491.

¹⁴ Norbert Peabody, 'Colonial Surveillance in British India: The Creation of the Intelligence Bureau' (1999) Modern Asian Studies 33(3) 649.

¹⁵ David Arnold, 'Policing the Colonial Body: Surveillance and the State in British India' (1994) History Workshop Journal 47 34.

¹⁶ David Arnold, 'Policing the Colonial Body: Surveillance and the State in British India' (1994) History Workshop Journal 47 34.

After independence, the India Witnessed the paradigm shift towards the digitalization and well structure technologies¹⁷ with the rise of digitalization that leads to the emerging use of digital surveillance by administrative authorities for the data control and impose limitation on digital freedom.¹⁸ In Post independence era, the India digital surveillance is managed by some enactments like Indian Telegraph Act, 1885, Information Technology Act 2005, Bhartiya Nyaya Sanhita, 2023 and the Data Protection Act.¹⁹ The statutes provide for the prior approval from the competent authority for any interception and make data fiduciary the laws provide for the transparency in surveillance scope of the absence of accountability of data stored. Permanently by the government agency. Additionally, with these legislations, the government established some intelligence agencies like National Technical Research organization and systems like Central Monitoring System gave the state to directly the power to access to the communication network with these the cell. Investigation Bureau, the research agency wing was established that were entrusted with the duty to collect intelligence data and monitor both internal and external threat to the national security²⁰, but with increase in the power of this agency create the threat.

Over the privacy of an individual Freedom as provided under the constitution India, but the difference in the laws made by the British government and the laws made by the Indian government was that the British were laws were more centric to maintain control over the citizens rather than to protect their rights and the Indian laws serve the purpose such as public order and national security.

III. JUDICIAL EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

The right to privacy has become one of the most significant constitutional rights in India which

provides the strong legal backing in the era of advanced technology which increasingly shared personal professional and social life. The constitution does not explicitly use the term privacy the idea has gradually been recognised through judicial interpretation. The primarily discussion on privacy emerged in Kharak Singh's case in which the Apex Court examined whether continuous police surveillance violated the individual's right to personal liberty, although the court did not expressly identify privacy as a distinct fundamental right at that time it struck down certain intrusive surveillance practices, it became significant for the future that privacy is inseparable from personal liberty and the one cannot enjoy liberty without having a private realm which is free from Interference. Even though the majority judgment was aware about this case marked the beginning of privacy debate in India.

The Supreme Court continued to develop the idea of privacy in later judgements in Gobind V. State of Madhya Pradesh,²¹ in this the court said that privacy does not form part of fundamental rights even though it may not be absolute. It focused that privacy evolves in societal changes and should be recognised within the meaning of liberty. Further, in R. Rajagopal v. State of Tamil Nadu,²² the court recognised that the privacy is right of individuals to protect their personal life from unwarranted publication by the media, this case also expanded privacy beyond surveillance and acknowledged that individuals deserve protection from unwanted exposure in the public sphere. All these decisions eventually covered the way for the historic nine-judge bench ruling in the case of Justice K.S. Puttaswamy, the court held that privacy is a fundamental right given by the Constitution of India, this ruling set privacy as an essential constitutional value and emphasized that it forms the basis of human dignity, personal liberty and individual autonomy.

The Puttaswamy's judgment made it clear that privacy is not a narrow concept it is a broad right that includes

¹⁷ Shruti Tripathi, 'Surveillance in India: Historical Roots and Contemporary Frameworks' (2020) *Journal of Indian Public Policy Review* 2(1) 55.

¹⁸ Anushka Kaushik, 'From Colonial Surveillance to Digital Authoritarianism: The Evolution of State Monitoring in India' (2021) *Journal of South Asian Studies* 44(4) 612.

¹⁹ Apar Gupta, 'Surveillance Reform in India: The Need for a Rights-based Framework' (2019) *Indian Journal of Law and Technology* 15 1.

²⁰ Anupam Chander, 'Surveillance in India: The Central Monitoring System and Beyond' (2014) 10(2) *Indian Journal of Constitutional Law* 113

²¹ 1975 AIR 1378

²² 1995 SCC (6) 632

the ability to make personal decisions, maintain control over one's body and preserve personal spaces. The court identified several aspects of privacy such as bodily privacy, spacious privacy and decisional privacy, bodily privacy which safeguards the individuals against unwanted physical intrusion, spacious Privacy protects private spaces such as the home and the decisional privacy which ensures that individuals have the freedom to make choices relating to their personal and intimate life.

The Puttaswamy's decision emphasised the nature of fundamental rights, the court observed that privacy strengthens the right to equality because it prevents arbitrary and discriminatory actions by their state. When individuals have fear of surveillance they are deprived to express themselves freely or participate fully in public life. Privacy operates as a safeguard that strengthens other freedoms which is given under constitution and ensure the citizens can exercise their rights without fear. The judgement also recognised communicational privacy which ensures personal communication whether digital or otherwise cannot be assessed or monitored without lawful decision. These protections are essential to maintain trust, autonomy and liberty in a digital society.

Due to rapid rise of technology, the court also found informational privacy as a crucial aspect of the right to privacy it refers to a person's control over their personal data how it is collected, stored, processed and shared. All over world where different organisations handle vast amounts of data, where individuals must have the right to protect their personal information from abuse.

In summary, the constitutional recognition of privacy under Article 21 represents a major shift in India's framework. This is from tentative beginnings in *Kharak Singh* to the powerful confirmation in *Puttaswamy*. The right to privacy has grown into a fundamental guarantee that protect human dignity personal freedom its link with Article 14 and 19 further illustrates that privacy is not a single right but an important concept that strengthens the overall structure of fundamental rights. As technology advances which continue to blur traditional boundaries. The constitutional foundation established by *Puttaswamy* provides strong framework for safeguarding personal autonomy in the modern era.

IV. LEGAL FRAMEWORK GOVERNING DIGITAL SURVEILLANCE IN INDIA

In recent years, India has experienced a major push towards digitalisation. Services that once depended on physical presence whether it was banking, updating official documents, taking medical advice, attending classes or applying for government benefits have gradually moved to online platforms, because of this shift both government bodies and private companies now collect huge amounts of personal data from citizens. The use of internet has expanded people have become increasingly concerned about issues such as unauthorised surveillance, frequent data leaks and the misuse of personal information.

As technology changed the state widened its powers of interception and monitoring but these powers were never organised into a single updated statute for these different laws govern like phone interception, digital monitoring and data protection. After the Supreme Court's ruling in privacy case held right to privacy became a fundamental right meaning every surveillance action must follow the principle of legality, necessity and proportionality. There are several laws and regulations enacted by Parliament for digital surveillance and individual privacy within this larger framework major laws shape India's surveillance system today such as Indian Constitution, 1950, the Indian Telegraph act 1995, the Information Technology Act, 2000, the Telecom Act, 2023 and the Digital Personal Data Protection Act, 2023.

1. Constitution of India, 1950 ²³

The Indian Constitution does not provide expressly Right to Privacy in its provisions but in this absence, the Supreme Court for the protection of individual guarantees the broader context of personal liberty. Which is starting from *Kharak Singh V. State of Uttar Pradesh* and later in decisions such as *Gobind V. State of Madhya Pradesh* and *R Rajagopal V. Union of India*, the Court recognised that privacy is closely linked to the dignity and autonomy of an individual. This position was finally settled by the nine-judge bench in *Justice K.S. Puttaswamy (Retd) V. Union of India* which held that the right to privacy is an integral part of Article 21 ensuring that every person enjoy a zone of personal freedom and the right to be alone.

²³ The Constitution of India, 1950, art. 21

In addition, Article 19(1) (a) protects the freedom of speech and expression, when state surveillance is excessive or unchecked can have a chilling effect in this freedom by discouraging individuals from speaking openly. Even so, this right is not absolute. Under Article 19 (2) the State may impose reasonable restrictions in areas such as national security, sovereignty and integrity and public order.

2. Indian Telegraph Act, 1885

The Telegraph Act introduced under colonial rule was designed to regulate how telegraph systems were created, managed and licensed while giving the government the power to lay and operate telegraph lines²⁴. The Act uses an unusually broad definition of the term Telegraph covering both wired and wireless communication due to this wide scope, the term naturally extends to later technologies such as telephones, wireless networks and mobile phones²⁵ even though these innovations emerged long after the law was enacted.

This act was written for Telegraph lines it continues to apply to the interception of telephone communication under Section 5(2), the government may intercept messages only in situations involving public emergency or threats to public safety and only for limited aims like national security, public order, preventing crime or preserving friendly relation with foreign nations. Courts have interpreted these powers very strictly in *PUCV V. Union of India*²⁶ the Supreme Court held that interception cannot be used for everyday investigations and must be connected to a real emergency. Likewise, the Bombay High Court in *Vinit Kumar V. Central Bureau of Investigation*²⁷ cancelled interception orders in bribery case, stating that no emergency conditions were present.

Following this ruling, Rule 419A was introduced to the Indian Telegraph Rules, it requires approval from the Home Secretary, written reasons, a time limit of 60

days, review by an oversight committee and destruction of intercepted material where no longer needed. However, despite the safeguards the process is still controlled entirely by the executive without any judicial supervision. In 2014, the government amended 419 A of the Telegraph Rules to include some safeguards against²⁸ unauthorised interception.

3. Information technology Act, 2000

The Information Technology Act was enacted to promote India's digital era by recognising electronic transactions and creating rules for online communications, cyber security and the functioning of the digital space. A major amendment was made in 2008 after Mumbai terror attacks. This gives the government's power to intercept, monitor and decrypt digital communication and allowed scrutiny of internet traffic.

With the shift to digital communication, the IT Act set up mechanism for monitoring electronic data section 69 allows the government to order interception, monitoring or decryption of electronic information on grounds search as national security, sovereignty, public order and crime prevention. This Act provides the Central Government the power to direct any agency of Government and if the intermediary fails to comply with this provision shall be punishable under this Act²⁹ and also provides the power to collect and monitor traffic data for the enhancing cybersecurity³⁰. The Act provides the power to officers of Central and the State Government to enter any public place, search and arrest without warrant to any person suspected of committing offence under this Act.³¹ The 2009 IT Rules outline how such orders must be issued reflecting a process similar to the Telegraph Act's model. Under this law intermediaries must help with decryption only if they control the encryption system or have access to the keys. They are not required to weaken end-to-end encryption. The debate intensified

²⁴ The Telegraph Act, 1885, s.4

²⁵ Indian Telegraph Act, 1885 s. 3(1AA). "telegraph" means any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means. Explanation. "Radio waves" or "Hertzian waves" means electro-magnetic waves of frequencies lower

than 3,000 giga-cycles per second propagated in space without artificial guide.

²⁶ AIR 1997 SC 568

²⁷ MANU/MH/2931/2019

²⁸ G.S.R. 18, Indian Telegraph (1st Amendment of 2014) Rules, 2014, (28 January 2014)

²⁹ The Information Technology Act, 2000, s. 69A

³⁰ The Information technology Act, 2000, s. 69B

³¹ The Information Technology Act, 2000, s. 80

after the 2021 Intermediary Guidelines, which require major messaging platforms to identify the first originator of a message. Many critics argue that this could undermine encryption and several challenges are still pending in court.

4. Telecom Act, 2023

The telecom Act, 2023 replaces older terminology and expands regulatory coverage to include internet-based communication services. Although it updates the framework it retains wide interception powers and authorised suspension of telecom services when public order concerns arise. What worries many observers is that the Act does not include judicial warrants or independent oversight bodies. The broad national security exemptions and strong executive control raise the possibility of misuse.

5. Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 grants protection of personal data of individuals and with consent data given protection regime and grants individuals certain rights such as data access, correction, grievance redressal, and purpose- specific processing. However, the act also carries significant exemptions particularly for government bodies.

The Act exempts public authorities and government from most obligations and gives the right in the name of State sovereignty and integrity, public order, safety, crime prevention because of these the act is limited in its ability to restrain surveillance activities by the state.

V. CONSTITUTIONAL STANDARD: THE PROPORTIONALITY TEST AND ITS APPLICATION TO SURVEILLANCE

1. Legality- although targeted interception is covered by the Telegraph Act and IT Act, large surveillance systems like the Central Monitoring system (CMS) and NETRA do not rest on clear, specific laws. They function mainly through internal government decisions license requirements reducing transparency.
2. Legitimate Aim -objective searches for protecting national security preventing crime or legitimate state aims so this requirement is usually met.

3. Rational Nexus- targeted surveillance can help achieve this aim, however weather bulk surveillance tools designed to scan or store massive amounts of data have a reasonable connection to these aims is still heavily debated.
4. Necessity- there is no judicial warrant requirement, no independent oversight authority and limited transparency around how surveillance powers are used. Since less intrusive methods exist such as targeted surveillance supervised by courts, it is unclear why broad executive-led systems are needed.
5. Balancing- the current framework tilts strongly in favour of the State individuals do not receive notice of interception and have minimal remedies and the DPDP Act exemptions reduce accountability ³² even further. Without independent checks the balance between security and privacy becomes difficult to maintain.

VI. DOCTRINE OF PROPORTIONALITY IN INDIA

The evolution of digital surveillance to be used as a tool by the investigating authorities to combat with the crime in digital world leads to the deteriorating effect on the fundamental rights of an individual. To challenge the state action in contravention of fundamental rights, court applies the doctrines of proportionality to resolve the conflict in such matters. The concept of the doctrine underlines that actions of the executive should be in restrictive nature and allows to invade into the privacy only when there is absolute necessity in the public interest. The doctrine ensures that the discretionary power entrusted to the law enforcing authorities should not be used arbitrarily, which would result in the violation of the privileges guaranteed to the people.

In democratic country like India, the courts have the power to review the state's actions under the guidance of the grand norm law under which the Supreme court of India under article 32³³ of the Indian constitution and the High Court Of the states under Article 226³⁴ respectively, have the power to apply the doctrine of Proportionality to review the states action. The application of the doctrine ensures the maintain of

³² Digital Personal Data Protection Act, 2023, s.17

³³ Constitution of India, Art 32

³⁴ Constitution of India, Art 226

harmony between the rights and the obligations of the state.

However, the unreasonable³⁵ action of the state was previously determined by the Wednesbury doctrine propounded by Lord Diplock it states that Wednesbury unreasonableness as a principle that applies to a decision is so illogical or morally unacceptable that no reasonable or sensible person after proper thinking over the issue, the doctrine was first time evolved in the case of *Associated Picture House v. Wednesbury Corporation*³⁶. The purpose of the application of the doctrine by the UK government was to limit the power of judicial review by the courts and to avoid unnecessary intervention in the state's autonomy. Ironically, since India Conquered by the British regime since decades it became one of the common wealth country, the governance leaves the resonating effect on India's administrative law.

The doctrine was initially developed from the Wednesbury reasonable test and now has been replaced by the doctrine of proportionality which offer a strict taste for legitimate aims, sustainability, necessary and balanced approach of states action³⁷. The court of law may interfere in the actions through judicial review the doctrine is applied in pursuit for the protection of fundamental right.

The Judicial review plays a vital role in the system of check and balance to enable the government to use its power in the prescribed limit, courts apply different ways to check whether administrative decisions are fair and lawful and also to determine whether the steps taken by the government is arbitrary in nature in the light of national security. The doctrines are applied in different situation the administrative actions are determined by the Wednesbury unreasonableness test and the proportionality test, Wednesbury test is usually strict and very deferential in nature which means the Courts may intervenes only when a decision is completely unreasonable. On the other sides

proportionality looks more closely at whether the government balanced different interest properly and whether its actions were really necessary especially when the rights are at stake.³⁸

In the English case *R v. Secretary of State for the Home Department*,³⁹ the House of Lord observed that sometimes the Wednesbury and proportionality test give the same result but proportionality involves more deeper and structured examination detailed instead of just checking whether the decision is irrational, it also scrutinize whether the decision maker actually balanced interest of the persons and whether the action of the state was truly necessary for the aim they wanted to pursue. Several scholars opined that Wednesbury should be kept for circumstances where the courts want to give more freedom to the government while the proportionality should be applied where rights are seriously affected⁴⁰.

In India the apex court has ruled that the doctrine of proportionality is applied when government actions are challenged on the ground of violating the Golden triangle of the fundamental rights, that is Article 19⁴¹ or 21⁴² and Article 14⁴³ of the constitution when a person claims discrimination under article 14, the court uses primarily review in which it examines the states action more closely to, check whether these are reasonable classification and whether the restriction is proportionate to the state action. However, when the action is challenged only on the ground that the action is arbitrary especially in services related matters like disciplinary punishments the court generally follows a second review based on the Wednesbury Standard.

Since no core fundamental freedom is involved in all these conditions, the proportionality test generally checks three things. First, whether the state's measure is suitable for its goal, which means whether they are proportionate second, whether it is necessary with no less restrictive option available and lastly whether the approach is not excessive for the persons affected this

³⁵ Ajoy PB, Administrative Action and the Doctrine of Proportionality in India (2012) 1 IOSR Journal of Humanities and Social Science 16

³⁶ *Associated Picture House v. Wednesbury Corporation* (1948) 1 KB 223 (CA)

³⁷ Apporva Anand, Revising the Wednesbury Standard: A Study on Reasonableness and Judicial Restraint (2024) 7 Indian Journal of Law and legal Research 2163

³⁸ Hamaad Muatafs Wednesbury Proportionality and Judicial Review (2014) LUMS Law Journal.

³⁹ *R v. Secretary of State for the Home Department* (2001) UKHL

⁴⁰ Veena Srirangam, A difference in Kind- Proportionality and Wednesbury (2016) 3 (1) IALS Student Law Review.

⁴¹ Constitution of India, Art 19

⁴² Constitution of India, Art 21

⁴³ Constitution of India, Art 14

shows that proportionality test in India works with different levels of scrutiny depending on the nature of the government action which means then application of the doctrine has multiple variation based on the interpretation of judicial mind⁴⁴. The doctrine of Proportionality is meant to restrain state surveillance but its application in India remains inconsistent and varied from case-case courts interpret these four steps differently.

VII. JUDICIAL REVIEW AND ADMINISTRATIVE DISCRETION

Administrative law in India plays a crucial role which ensuring that the executive exercise its powers within constitutional limits. Judicial Review is the doctrine of ultra vires and principles of natural justice simultaneously form the backbone of this control. These doctrine highlights how administrative mechanisms must balance governance needs with the protection of individual rights in contemporary issues such as surveillance.

Administrative powers are divided into ministerial and discretionary powers. Ministerial powers establish strict compliance with statutory directions and discretionary powers allow authorities to act based on their judgment. This discretion is essential for governance if this discretion not checked properly then it becomes arbitrary. Judicial Review acts as a constitutional safeguard to ensure that administrative discretion remains lawful, rational and procedurally fair. The objective of judicial review is not substitutes the administrative authority's but to assess whether the decision-making process is legal and reasonable. Judiciary intervenes when actions are arbitrary, ultra vires, violates principles of natural justice or shows non-application of mind. The Indian Apex Court has repeatedly emphasized that the unchecked discretion threatens the rule of law. The Court held that the absolute discretion contradicts constitutional principles and be subject to judicial scrutiny.⁴⁵

There are several grounds for administrative discretion have evolved through judicial decisions. Discretion may be invalidated for considering irrelevant factors,

ignoring relevant considerations, acting for improper purposes or exercising power mala fide, there are other justifiable interventions such as jurisdictional errors, colourable exercises of power and breach of natural justice.

VIII. DOCTRINE OF ULTRA VIRES

The doctrine of ultra vires means an authority must act within limit of its powers which is central to judicial control. If actions are taken beyond statutory authority or in violation of procedural requirements are void. In India, ultra vires covers illegality, irrationality and procedural impropriety. In ruling the Supreme Court held that judicial review focuses on the decision-making not merits. Likewise, the notes that arbitrariness, mala fide or abuse of power are sufficient grounds to invalidate administrative actions.⁴⁶ These principles guarantee that discretionary actions is fair and constitutionally accountable.

Despite the general availability of judicial review in administrative law its application to surveillance decisions is limited. Presently, law does not require a judicial warrant before interception. Further, individuals not have knowledge that they have been shrivelled making it impossible to challenge orders. This undermines has two key purposes of judicial review is accountability and redress. Though India Judiciary retain the power to review surveillance actions, secrecy, lack of notice and classified procedures effectively act as informal ejective clauses. After the Puttaswamy judgment recognises privacy as a fundamental right, surveillance laws still lack efficient procedural safeguards or judicial checks.⁴⁷ Rule of law principles establish that government power be exercised transparently, predictably and with accountability. However, India's surveillance framework gives broad discretion to the executive with minimal external constraints conflicting with this principle. A well-known scholarly position states that interference with rights must be subject to effective control which is normally assist by judicial bodies.⁴⁸ The two important natural justice principles- the right

⁴⁴ Ibid 16

⁴⁵ Baldev Raj V. Union of India

⁴⁶ Tata Cellular V. Union of India (1994) 5 SCC 651; A.P. V. McDowell & Co. (1996) 3 SCC 709

⁴⁷ V Bhandari & K Lahiri, "The Surveillance State, Privacy and Criminal Investigation in India" (2023)

⁴⁸ Scholarly commentary from OSR Journal of Humanities & Social Science (2012)

to be heard and rule against bias are entirely absent in surveillance procedures. Since individuals are never informed or allowed to contest surveillance orders and because review is carried out by bureaucrats who also authorize the orders the system fails to satisfy basic fairness requirements. Indian Administrative law is increasingly constitutionalized means courts test administrative action against fundamental rights standards. This implies that surveillance practices should also review under compliance with Article 14, 19 and 21.

There are certain policy and reforms formulated by scholars and policy groups to link India's Surveillance with Administrative law standards such as judicial authorisation of interception orders before surveillance is conducted, independent oversight authority including judicial and parliamentary representation, procedural safeguards such as notice, appeal rights and destruction protocols and transparent reporting to Parliament the public on aggregate interception data.

IX. JUDICIAL DECISIONS SHAPED BY THE DOCTRINE OF PROPORTIONALITY

In several landmark judgements, where Supreme Court emphasised and developed the application of the doctrine of proportionality in India in the privacy case in which the court recognises the right to privacy as a fundamental right and made it clear that the state must satisfy the four steps proportionality test before restricting this right that is legality, legitimate aim, necessity and proportionality in strict sense.

The test was first systematically let down in the *Modern Dental College & Research Centre v. State of Madhya Pradesh*⁴⁹, where the court relied on comparative principles from German constitutional law to assess proportionality in administrative action. Similarly in the case *Anuradha Bhasin v. Union of India*⁵⁰, the court applied the proportionality doctrine to evaluate restriction on internet access in Jammu and

Kashmir holding that indefinite shutdown is unconstitutional and must meet the restrict necessity requirement. In another significant case of *Reserve Bank of India v. Cryptocurrency Exchanges*⁵¹ in which the court struck down RBI's circular holding that measures were excessive and not supported by evidence. Analysing these Judicial decisions is clear that proportionality has become an essential standard for reviewing the state actions, although varied interpretation continues to evolves and creating some uncertainty in administrative law.⁵²

X. OPERATIONAL DIMENSIONS OF STATE SURVEILLANCE IN INDIA (CMS, NETRA, NATGRID)

India has increased the reliance on digital surveillance as a tool to ensure the national security and for the maintenance of public order and investigate cyber related crimes and surveillance functioned at multiple levels in investigation process such as the macro level mass monitoring and micro level targeted interception operates and at the macro level the state deploys technologies like CCTV's, facial recognition cameras and lateral surveillance programs.

The country's capital leads globally in the Density of surveillance cameras with over 1800 cameras per square mile, surpassing various global leaders such as Beijing and London while Chennai and Mumbai ranked at 3rd and 18th respectively. The Delhi government recently gear up Phase two of its CCTV project aiming to install 140,000 Additional campus lateral surveillance initiatives such as Cyber Volunteers Program by the Indian Cyber Crime Coordination Centre encourage citizens to report unlawful online activities. During Covid 19 pandemic India witnessed the immense use of digital surveillance to combat with the virus some online platforms were used like Arogya Setu app and Quarantine to avoid the involvement of any human agent.⁵³

⁴⁹ *Modern Dental College & Research Centre v. State of Madhya Pradesh* (2016) 3 SCC 1.

⁵⁰ *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637.

⁵¹ *Reserve Bank of India v. Cryptocurrency Exchanges* (2020) SCC Online SC 1234.

⁵² Apar Gupta, 'The Right to Privacy in India: Emerging Issues in Digital Surveillance' (2021) 16(1) *Indian Journal of Law and Technology* 45 <https://vidhilegalpolicy.in> accessed 2 December 2025.

⁵³ Shekar K& Mehta S. *The State of Surveillance in India: National Security at the Cost of Privacy?* (2025)

At the micro level, targeted surveillance occurs through lawful interception systems integrated into telecom and Internet networks under license granted to government agencies. Some systems like the Centralised Monitoring System (CMS), Network traffic analysis (NETRA) National Intelligence Grid (NATGRID) and lawful Interception and Monitoring⁵⁴. These monitoring systems enable real time, monitoring of phone calls, messages, emails and social media activity social media networking tools and AI driven analytics track misinformation and potential threats, while facial recognition⁵⁵ systems and other linked database provide additional tracking capabilities.

But the challenge that Indian surveillance system faces is the mechanism operates without a strong data protection framework. The Pegasus spyware Incident revealed that unauthorised hacking and surveillance could occur without the target's knowledge⁵⁶ which is usually happened with senior citizens and the children engaged in online gaming platforms, while interception is legally authorised under the Information Technology Amendment Act, 2008, Section 43⁵⁷ and 46⁵⁸. The act does not provide the explicit definitions of sub terms like suspect or suspicious activity this give the authorities misuse their powers arbitrarily consequently encroaches the of privacy of citizens, these sections penalise unauthorised access and set up adjudicating authorities but the statue is silent to apply any limitation surveillance, this gap allows the state to use wide discretionary power without any formal checks there is no mandatory prior judicial authorization or independent review.

XI. GLOBAL APPROACH TO REGULATING STATE SURVEILLANCE: A COMPARATIVE OVERVIEW (UK, USA, EU)

These days, surveillance has become a major tool used by the government authorities to ensure public safety especially with the rise of advanced technologies such as Artificial Intelligence, facial recognition and biometric system. Different countries regulate these tools in differently based on their social, legal and political structures while some nations have strict and transparent rules to protect privacy, fairness and accountability.

In the United Kingdom the surveillance system is govern by the Investigatory Powers Act which provides that all forms of surveillance must be proportionate, necessary and justified. Authorities cannot monitor individuals arbitrarily, they must show a real threat or risk before accessing someone's data they must obtain judicial independent approval, which act as a strong layer of check and balance. The role of the investigatory power commissioner and judicial commissioner conduct regular audits regularly to avoid privacy invade by the authorities of citizens⁵⁹. This kind of institutional oversight helps to prevent misuse and build public trust. Compared to this, India's Surveillance System lacks similarly strong and independent review body and regulate the high- risk surveillance operations.

In European Union Surveillance law is based on strict adherence to data protection laws under the General Data Protection regulation, the act provides very strict protection for high risk personal data, such as biometric information or data from wearable devices any system that might violates on personal privacy must go through a data protection impact assessment

law Foyer International Journal of Doctrinal Legal Research, Volume 3

⁵⁴Kamalpreet Kaur, 'Digital Surveillance and Indian Privacy Laws' (2025) 3(1) Law Foyer International Journal of Doctrinal Legal Research <https://www.ijdlr.com> accessed 2 December 2025.

⁵⁵ S.B. Thorat, S.K. Nayak and Jyoti P. Dandale, 'Facial Recognition Technology: an analysis with scope in India' (2010) <https://arxiv.org/abs/1005.4263>

⁵⁶ Shreshtha Menon, 'Surveillance Laws in India in light of the Pegasus Project' (2021) 4(5) International Journal of Law Management & Humanities 1011–

1019 <https://ijlmh.com/paper/surveillance-laws-in-india-in-light-of-the-pegasus-project/> accessed 2 December 2025.

⁵⁷ Information Technology Act, Section 43

⁵⁸ Information Technology Act, Section 46

⁵⁹ Martin Husovec, "Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace" (2022) International Data Privacy Law <https://academic.oup.com/idpl/article/12/4/276/6668508> accessed 2 December 2025.

(DPIA) through this process authorities must advocate why they need certain data and why less intrusive alternatives are not suitable⁶⁰.

In the United States of America surveillance is shaped by the fourth Amendment which protects individuals from unreasonable search and seizure. After 9/11 Patriot Act expanded government surveillance powers the experts have cautioned that such wide powers affect the constitutional protection.⁶¹ This shows India that while security is important right should not be ignored any surveillance system must include clear limits, approval process and accountability mechanism.

The Indian Surveillance System faces several loopholes when compared to the surveillance systems in the developing countries. India has adopted technologies like Aadhaar linked biometrics, Facial recognition pilots and AI based monitoring system but have face several gaps in them. First, the country lacks a strong independent oversight bodies like the Investigatory powers (UK) or Data Protection Supervisory Authorities (EU). Second, the ethical safeguards and anti-bias protection remain weak, which raise the risk of discriminatory or excessive surveillance.

India does not consistently enforce necessity and proportionality test before applying the high-risk technologies unlike the European Union or the United Kingdom frameworks meaning privacy would be compromised without clear justification. Moreover, it does not provide any provision for mandatory impact assessment mythical reviews before launching any new surveillance system. The transparency is also limited, so the public and policy maker may not fully know how data is collected and stored used but they are some recommendations which India can borrow

from these developing countries to strengthen their digital surveillance system to beat the digital world in the modern era.

The UK, European Union and USA are some of the developing countries which assert that their surveillance systems are strong. These are some ways by which the India may formulate an effective legislation to deal with digital surveillance in conflict with privacy right first, establish a strong independent body to check an order in surveillance system so that the arbitrary actions can be examined. Second, any surveillance must pass necessary and proportionality test to make sure that it's really needed and is not violative to the privacy of the people.⁶²

Also, impact assessments like the United Nation Development programme (UNDP) should be done before deploying any new technology in surveillance and procedure and international rules like International Covenant on Political Right (ICCPR) and Article 7 and General Data Protection Regulation principles suggest that limiting data collection using it only for proper person and letting people correct or delete their data. Finally, transparency and reporting can build trust and make sure that the system stays accountable.

XII. GAPS, LOOPHOLES AND STRUCTURAL CHALLENGES IN INDIA'S SURVEILLANCE LAWS

India surveillance system continues to be governed by colonial era and early digital statutes such as the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 the absence of a unified, modern surveillance law means that interception powers remain fragmented across multiple legislations this

⁶⁰ Stuti, "Balancing Data Privacy: A Comparative Analysis of International and National Legal Frameworks for Data Protection and Surveillance" (IJA LR, Vol 4, Issue 4, 2024) <https://ijalr.in/volume-4-issue-4/balancing-data-privacy-a-comparative-analysis-of-international-and-national-legal-frameworks-for-data-protection-and-surveillance-stuti/> accessed 2 December 2025.

⁶¹ Daniel J Solove, "The Digital Fourth Amendment and National Security" (2019) Journal of National Security Law & Policy

<https://jnsplp.com/articles/digital-fourth-amendment/> accessed 2 December 2025.

⁶² Darshita, "Surveillance, Bias and Human Rights: The Case of Facial Recognition" (2024) International Journal of Human Rights Law Review <https://humanrightlawreview.in/wp-content/uploads/2024/09/Surveillance-Bias-and-Human-Rights.pdf> accessed 2 December 2025.

patchwork framework does not satisfy the constitutional requirement of a clear, specific and accessible legal basis especially after the recognition of privacy as a fundamental right.

1. Absence of unified and modern surveillance law
India does not have a single statute that regulates both analogue and digital surveillance instead interception powers are dispersed across outdated laws resulting in overlapping standards and inconsistent safeguards the Telegraph act a colonial statute originally meant for Telegraph lines continues to regulate modern telephone interception courts have repeatedly emphasised that the right to privacy demands a precise and transparent legal framework something the current structure fails to provide.

2. Executive controlled interception without judicial oversight

A major flaw in the current system is a complete absence of judicial supervision all interception orders are issued, reviewed and renewed internally by the executive this stands in contrast to democratic practices worldwide where independent judicial authorization is mandatory although the Supreme Court has expressed concerns about unchecked executive power and has insisted on procedural safeguards these safeguards remain internal and lack transparency living significant room for misuse

3. Lack of transparency and public accountability

India does not release annual interception statistics oversight reports or audit findings large surveillance initiatives such as central monitoring system, NATGRID and NETRA operate without public disclosure or independent scrutiny this opacity conflicts with the principle of proportionality which requires that any intrusion into privacy must be accompanied by accountability and minimal invasion.

4. Broaden and vague national security clauses

Key terms such as public emergency, public safety, security of the state and sovereignty in Section 5(2) to the Telegraph act and section 69 of the IT act are extremely broad and undefined. In Vineet Kumar v. CBI, the Supreme Court criticised the mechanical use of these grounds to justify interception even when no real emergency existed such vague clauses turn what should be exceptional measures into routine practices enabling excessive surveillance.

5. Wide Government exemptions under Data Protection Act, 2023

Although the Data Protection Act 2023 establishes a strong structural framework section 17 empower the central government to exempt any public authority from most obligations on grounds such as national security, public order these broad exemptions undermine the protective purpose of the act and dilute privacy safeguards weakening the very framework that was expected to enhance accountability

6. No Notice no remedies and weak oversight

Individual subjected to surveillance are never informed not even after the period of interception is over there are no meaningful remedies or independent complaint mechanisms available review committees under the Telegraph and IT rules consist entirely of executive officials offering no impartial oversight this violates the principle that any rights restrictive measures must ensure accessible and effective redress.

7. Absence of safeguards against mass surveillance

While Indian law formally authorises only targeted surveillance systems such as CMS enable bulk and centralised monitoring of communication data. these systems can collect information on millions of users without specific warrants or individual suspicion effectively enabling mass surveillance without adequate legal safeguards.

XIII. CONCLUSION

The growing use of digital surveillance in India gives a significant constitutional concern about the limits of State power in society. With modern technologies making it easy for authorities to monitor individuals and store their data and track their activities raises concern about privacy have become stronger. Simultaneously, the Supreme Court's affirmation of privacy as a part of Article 21 imposes a strict responsibility on the State to justify any interference which proving that the action is legal, essential and limited in scope. This continuing tension between individual freedom and administrative authority forms the core of today's legal concerns.

The doctrine of proportionality is important to resolving this issue and it requires the government to carefully examine each step which takes while restricting fundamental rights and ensures the

measures are not exhaustive. Judicial decisions including Puttaswamy, PUCI and Anuradha Bhasin show that courts now expect higher levels of accountability and stronger procedural safeguards before accepting surveillance in any form. Currently, the surveillance governs by existing laws such as Telegraph Act, the IT Act and the Telecom Act which grants wide powers for the independent supervision. This imbalance makes the urgent need of reforms. India requires a strong transparent surveillance authorisation, clearly defines the term national security and supervise bodies that operate independently rather than executive control. As governance becomes more digital, it is vital that these systems operate within constitutional boundaries. A surveillance framework comes from proportionality will not only protect individual liberty but also strengthen public confidence in democratic institutions.

XIV. RECOMMENDATIONS FOR BUILDING A RIGHTS- PROTECTIVE SURVEILLANCE FRAMEWORK

India's surveillance framework now needs a shift from fragmented executive driven mechanism to a consolidated structure which exclusively defines the circumstance and limits under which the state may collect personal data. Such law must include mandatory judicial warrants for interception replacing the current executive only approval system weakens constitutional safeguards

Reforms to the Data Protection are important the government exemptions under section 17 should be narrowed subject to necessity and proportionality test and paired with stronger rights for individuals including notice wherever possible and effective grievance mechanisms

India should shift towards targeted intelligence-based surveillance rather than large scale data collection. Strengthening cyber security, promoting privacy by design technologies and training officials in lawful interception practices will help balance National Security with constitution privacy.

REFERENCES

[1]. Government of India. 1950. Constitution of India. Government of India Press, New Delhi.

- [2]. The Indian Telegraph Act, 1885. Government of India, New Delhi.
- [3]. The Information Technology Act, 2000. Government of India, New Delhi.
- [4]. The Information Technology (Amendment) Act, 2008. Government of India, New Delhi.
- [5]. The Indian Post Office Act, 1898. Government of India, New Delhi.
- [6]. The Indian Penal Code, 1860. Government of India, New Delhi.
- [7]. The Code of Criminal Procedure, 1973. Government of India, New Delhi.
- [8]. Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023. Government of India, New Delhi.
- [9]. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. Unique Identification Authority of India, New Delhi.
- [10]. [10] The Digital Personal Data Protection Act, 2023. Government of India, New Delhi.
- [11]. [11] The Telecom Act, 2023. Ministry of Communications, Government of India, New Delhi.
- [12]. [12] The Criminal Tribes Act, 1871 (Repealed). Government of India, New Delhi.
- [13]. [13] The Police Act, 1861. Government of India, New Delhi.
- [14]. [14] Supreme Court of India. 1962. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
- [15]. Supreme Court of India. 1975. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
- [16]. Supreme Court of India. 1994. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
- [17]. Supreme Court of India. 1996. People's Union for Civil Liberties (PUCI) v. Union of India, (1997) 1 SCC 301.
- [18]. Supreme Court of India. 2017. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- [19]. Bombay High Court. 2019. Vinit Kumar v. Central Bureau of Investigation, 2019 SCC OnLine Bom 3155.
- [20]. Supreme Court of India. 2016. Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
- [21]. Supreme Court of India. 2020. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

- [22]. Supreme Court of India. 2020. Reserve Bank of India v. Internet and Mobile Association of India, (2020) 10 SCC 274.
- [23]. House of Lords (UK). 1991. R v. Secretary of State for the Home Department, ex parte Brind, [1991] 1 AC 696.
- [24]. Court of Appeal (UK). 1948. Associated Provincial Picture Houses Ltd. v. Wednesbury Corporation, [1948] 1 KB 223.
- [25]. Supreme Court of India. 1952. Commissioner of Police v. Gordhandas Bhanji, AIR 1952 SC 16.
- [26]. Supreme Court of India. 1967. Barium Chemicals Ltd. v. Company Law Board, AIR 1967 SC 295.
- [27]. Supreme Court of India. 1970. Gell v. Teja Noora, AIR 1970 SC 1269.
- [28]. Ministry of Home Affairs. 2011. National Intelligence Grid (NATGRID) Framework Document. Government of India, New Delhi.
- [29]. Ministry of Home Affairs. 2014. Central Monitoring System (CMS) Overview. Government of India, New Delhi.
- [30]. Defence Research and Development Organisation. 2013. NETRA (Network Traffic Analysis System) Programme Overview. Government of India.
- [31]. Ministry of Electronics and Information Technology. 2020. Aarogya Setu Mobile Application Documentation. Government of India, New Delhi.
- [32]. Indian Cyber Crime Coordination Centre (I4C). 2021. Cyber Volunteer Program Guidelines. Ministry of Home Affairs, New Delhi.
- [33]. United Nations. 1990. UN Guidelines for the Regulation of Computerized Personal Data Files. United Nations, New York.
- [34]. European Union. 2018. General Data Protection Regulation (GDPR). Official Journal of the European Union, Brussels.
- [35]. Council of Europe. 2001. Convention on Cybercrime (Budapest Convention). Council of Europe, Budapest.
- [36]. United Kingdom Parliament. 2016. Investigatory Powers Act 2016. Her Majesty's Stationery Office, London.
- [37]. United States Congress. 2001. USA PATRIOT Act. Washington, D.C.
- [38]. United States Congress. 2018. CLOUD Act (Clarifying Lawful Overseas Use of Data Act). Washington, D.C.
- [39]. United Nations. 1966. International Covenant on Civil and Political Rights (ICCPR). United Nations, New York.
- [40]. United Nations Development Programme. 2019. Guidelines on Data Protection Impact Assessment. UNDP, New York.
- [41]. Daniel J Solove, "The Digital Fourth Amendment and National Security" (2019) Journal of National Security Law & Policy <https://jnslp.com/articles/digital-fourth-amendment/> accessed 2 December 2025.
- [42]. Darshita, "Surveillance, Bias and Human Rights: The Case of Facial Recognition" (2024) International Journal of Human Rights Law Review <https://humanrightlawreview.in/wp-content/uploads/2024/09/Surveillance-Bias-and-Human-Rights.pdf> accessed 2 December 2025.
- [43]. Ajoy PB, 'Administrative Action and the Doctrine of Proportionality in India' (2012) 1 IOSR Journal of Humanities and Social Science 16
- [44]. Apporva Anand, 'Revising the Wednesbury Standard: A Study on Reasonableness and Judicial Restraint' (2024) 7 Indian Journal of Law and Legal Research 2163
- [45]. Apar Gupta, 'Digital Surveillance and Privacy in India: Legal and Ethical Dimensions' (2021) 16 Indian Journal of Law & Technology <https://vidhilegalpolicy.in/wp-content/uploads/2021/06/IJLT-Vol-161.pdf> accessed 2 December 2025
- [46]. Apar Gupta, 'The Right to Privacy in India: Emerging Issues in Digital Surveillance' (2021) 16(1) Indian Journal of Law & Technology 45 <https://vidhilegalpolicy.in> accessed 2 December 2025
- [47]. Dr Rumi Dhar & Sonia Nath, 'Digital Surveillance and Civil Rights: Assessing the Impact on Privacy' (2024) 5(1) Chanakya Law Review 66
- [48]. Kamalpreet Kaur, 'Digital Surveillance and Indian Privacy Laws' (2025) 3(1) Law Foyer International Journal of Doctrinal Legal Research <https://www.lijdlr.com> accessed 2 December 2025

- [49]. Martin Husovec, 'Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace' (2022) *International Data Privacy Law* <https://academic.oup.com/idpl/article/12/4/276/668508> accessed 2 December 2025
- [50]. P. D. Prasannakumar, 'Reassessing the Indian Telegraph Act 1885 in the Light of the Right to Privacy' (2025) *Social Science Research Journal* <https://www.socialsciencejournals.net/archives/2025/vol7issue2/PartA/7-2-12-435.pdf> accessed 2 December 2025
- [51]. Shekar K & Mehta S, 'The State of Surveillance in India: National Security at the Cost of Privacy?' (2025) *Law Foyer International Journal of Doctrinal Legal Research*, Vol 3
- [52]. Shreshtha Menon, 'Surveillance Laws in India in Light of the Pegasus Project' (2021) 4(5) *International Journal of Law Management & Humanities* 1011–1019 <https://ijlmh.com/paper/surveillance-laws-in-india-in-light-of-the-pegasus-project/> accessed 2 December 2025
- [53]. Stuti, 'Balancing Data Privacy: A Comparative Analysis of International and National Legal Frameworks for Data Protection and Surveillance' (*IJA LR*, Vol 4, Issue 4, 2024) <https://ijalr.in/volume-4-issue-4/balancing-data-privacy-a-comparative-analysis-of-international-and-national-legal-frameworks-for-data-protection-and-surveillance-stuti/> accessed 2 December 2025
- [54]. S.B. Thorat, S.K. Nayak & Jyoti P. Dandale, 'Facial Recognition Technology: An Analysis with Scope in India' (2010) <https://arxiv.org/abs/1005.4263>
- [55]. Veena Srirangam, 'A Difference in Kind: Proportionality and *Wednesbury*' (2016) 3(1) *IALS Student Law Review*
- [56]. Daniel J Solove, 'The Digital Fourth Amendment and National Security' (2019) *Journal of National Security Law & Policy* <https://jnslp.com/articles/digital-fourth-amendment/> accessed 2 December 2025
- [57]. Hamaad Muatafs, 'Wednesbury Proportionality and Judicial Review' (2014) *LUMS Law Journal*
- [58]. Ujjwal Kumar Singh, 'Surveillance, Public Order and Colonial Governance in India' (2007) *International Review of Sociology* 17(3) 491
- [59]. Norbert Peabody, 'Colonial Surveillance in British India: The Creation of the Intelligence Bureau' (1999) *Modern Asian Studies* 33(3) 649
- [60]. David Arnold, 'Policing the Colonial Body: Surveillance and the State in British India' (1994) *History Workshop Journal* 47 34