

Section 69 of the Information Technology Act and the Right to Privacy: A Post-Puttaswamy Critical Analysis

Mr. Satish Ranawade¹, Miss. Megharani Nikam²

^{1,2} *Modern Law College, Pune.*

Abstract—The growth of digital communication has transformed both criminal investigation and the relationship between the individual and the State. Section 69 of the Information Technology Act, 2000 empowers the Central Government, State Government, or specially authorised officers to direct interception, monitoring or decryption of information through a computer resource on specified grounds.

The power serves legitimate interests such as national security, public order and investigation of offences, but its exercise may intrude deeply into privacy. The constitutional position changed decisively with the Supreme Court's nine-judge Constitution Bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India, which recognised privacy as a fundamental right protected under Article 21 and the wider scheme of Part III. This article examines Section 69 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 through the post-Puttaswamy requirements of legality, legitimate State purpose, necessity and proportionality.

It considers the continuing relevance of *People's Union for Civil Liberties v. Union of India*, executive authorisation, secrecy, collateral surveillance, decryption, data retention, freedom of expression and remedies. It argues that Section 69 cannot be treated as unconstitutional merely because it enables surveillance; however, the breadth of executive discretion and the limited nature of independent oversight require stronger safeguards.

The article proposes independent authorisation for highly intrusive surveillance, reasoned orders, strict time limits, data minimisation, purpose limitation, stronger review mechanisms and effective remedies. The constitutional objective should be neither unrestricted surveillance nor absolute immunity from investigation, but a system in which every serious intrusion into digital privacy is demonstrably lawful, necessary and proportionate.

Index Terms—Section 69; Information Technology Act, 2000; Right to Privacy; Puttaswamy; surveillance;

interception; monitoring; decryption; proportionality; Article 21; informational privacy.

I. INTRODUCTION

The digital environment has changed the character of modern criminal investigation. Evidence may now exist in electronic communications, cloud accounts, messaging platforms, social-media records, connected devices and encrypted systems. Crimes involving terrorism, organised crime, cyber fraud, trafficking and financial offences can leave digital traces that are difficult to obtain through conventional investigative methods. The State therefore requires lawful powers to obtain digital evidence and to protect national security.

At the same time, the scale and depth of digital information create a constitutional problem. A smartphone or computer may contain years of private correspondence, photographs, financial information, professional communications, location records, contacts and personal choices. Access to such information can expose not only the individual under investigation but also family members, colleagues and other persons who have no connection with the alleged offence.

Section 69 of the Information Technology Act, 2000 ("IT Act") occupies an important place in this framework. It permits interception, monitoring or decryption of information generated, transmitted, received or stored in a computer resource where the statutory requirements are satisfied. The provision operates with procedural safeguards prescribed by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.ⁱ

The constitutional problem is not whether the State can ever conduct surveillance. The more difficult question is the extent to which surveillance may be

permitted without violating the fundamental right to privacy. That question has acquired particular importance after Justice K.S. Puttaswamy (Retd.) v. Union of India, where a nine-judge Constitution Bench unanimously held that privacy is constitutionally protected as an intrinsic part of Article 21 and as part of the freedoms guaranteed by Part III.ⁱⁱ

Before Puttaswamy, the Supreme Court had already developed important safeguards. In *People's Union for Civil Liberties v. Union of India* ("PUCL"), the Court held that telephone tapping is a serious invasion of privacy and required procedural controls against arbitrary interception.ⁱⁱⁱ Puttaswamy, however, supplied a broader constitutional foundation, particularly through its recognition of informational privacy.

This article critically analyses Section 69 from that post-Puttaswamy perspective. It examines the statutory framework, the legality and proportionality requirements, executive authorisation, decryption, collateral surveillance, freedom of expression, retention of information and possible reforms. The central argument is that Section 69 should be interpreted as a controlled investigative power, not as an unrestricted gateway into private digital life.

II. STATUTORY FRAMEWORK OF SECTION

69

Section 69 of the IT Act authorises the Central Government or a State Government, or an officer specially authorised by the appropriate Government, to issue directions for interception, monitoring or decryption of information through a computer resource. The authority must be satisfied that the measure is necessary or expedient in specified interests and must record reasons in writing.^{iv}

The statutory grounds include the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, prevention of incitement to the commission of a cognizable offence relating to the specified interests, and investigation of an offence. The provision further permits the Government to require subscribers, intermediaries or persons in charge of computer resources to provide facilities and technical assistance.

The breadth of the provision is significant. It is not limited to the interception of a particular form of communication. Information may be generated, transmitted, received or stored in a computer resource. The provision therefore operates across a wide digital environment.

Section 69(2) places the procedural and safeguard requirements under prescribed rules. The 2009 Rules provide the operational framework for requests, authorisation, implementation, review and confidentiality. The existence of rules is constitutionally relevant because surveillance involves an especially serious interference with personal autonomy.

The provision should also be distinguished from Sections 69A and 69B. Section 69A principally concerns blocking public access to information, while Section 69B addresses monitoring and collection of traffic data for cybersecurity.^v Section 69 is therefore a distinct surveillance power directed at information itself.

The statutory scheme has a legitimate purpose. Criminal investigation would be seriously weakened if investigators could not lawfully obtain relevant electronic information. Nevertheless, a broad statutory power must be administered within constitutional limits. The expression "necessary or expedient" cannot be treated as a substitute for an actual assessment of necessity, and "investigation of an offence" should not automatically justify the most intrusive form of digital access.

A constitutional reading of Section 69 consequently requires attention to the nature of the alleged offence, the information sought, the expected investigative value, available alternatives, duration and safeguards for unrelated information.

III. DEVELOPMENT OF THE RIGHT TO PRIVACY BEFORE PUTTASWAMY

The constitutional recognition of privacy developed gradually through Indian judicial decisions. In *M.P. Sharma v. Satish Chandra*, the Supreme Court did not recognise a broad constitutional protection against searches.^{vi} *Kharak Singh v. State of Uttar Pradesh* similarly reflected uncertainty concerning whether privacy was independently protected by the Constitution.^{vii}

Later decisions moved towards stronger protection of personal liberty. The most important pre-Puttaswamy surveillance decision was *PUC v. Union of India*. The case concerned telephone tapping under Section 5(2) of the Indian Telegraph Act, 1885. The Supreme Court stated that telephone tapping is a serious invasion of privacy and held that telephone conversations within the privacy of the home or office fall within Article 21.^{viii}

The Court did not treat privacy as an absolute prohibition on interception. Instead, it required procedural safeguards. Among other requirements, interception orders were to be issued by specified senior authorities, copies were to be forwarded to review bodies, orders were subject to duration limits, and records were to be handled under prescribed safeguards.^{ix}

PUC is particularly relevant to Section 69 because it demonstrates a constitutional model in which surveillance may be legitimate but must be structured by procedural restraints. The judgment recognised the danger of technological eavesdropping and the possibility of abuse by governmental authorities.

The weakness of the pre-Puttaswamy position was that privacy lacked the comprehensive constitutional foundation that later became available. The question whether privacy was a fundamental right was settled decisively only in 2017.

Puttaswamy therefore did not create privacy from nothing. It consolidated and constitutionally elevated a principle that had emerged through earlier decisions. For Section 69, the significance lies in the fact that surveillance safeguards must now be understood as part of the protection of a recognised fundamental right rather than merely as administrative precautions.

IV. PUTTASWAMY AND INFORMATIONAL PRIVACY

Justice K.S. Puttaswamy (Retd.) v. Union of India fundamentally transformed Indian constitutional privacy law. The nine-judge Constitution Bench unanimously held that the right to privacy is protected as an intrinsic part of life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III.^x The Court overruled the contrary portions of *M.P. Sharma* and *Kharak Singh*.^{xi}

The judgment is particularly important because it recognised that privacy is multidimensional. It encompasses bodily privacy, spatial privacy, decisional autonomy and informational privacy. Informational privacy concerns an individual's interest in controlling personal information and protecting the individual from unjustified intrusion into personal data.

Digital technology magnifies the significance of informational privacy. Information that appears harmless when viewed separately can become highly revealing when aggregated. A record of location, contacts, searches, purchases and communications may disclose patterns of behaviour and relationships. Consequently, surveillance must be assessed not merely by asking what individual piece of information is obtained, but also by considering the cumulative picture created by access.

Puttaswamy also clarified that privacy is not absolute. Constitutional privacy can be restricted where the State satisfies the requirements applicable to limitations upon fundamental rights. The later proportionality jurisprudence gives practical structure to that inquiry.

For Section 69, the implication is substantial. The statutory existence of a surveillance power does not end constitutional scrutiny. The State must show a lawful basis and a constitutionally permissible objective, and the exercise of the power must be necessary and proportionate.

The recognition of informational privacy also means that digital surveillance deserves heightened attention where it concerns large volumes of information or information of an intimate nature. A request to intercept one narrowly identified communication and a request to access an entire digital device should not be treated as equivalent intrusions.

V. LEGALITY AS THE FIRST CONSTITUTIONAL REQUIREMENT

The first requirement for a privacy-infringing measure is legality. State surveillance must have a basis in law. Section 69 satisfies the formal requirement because Parliament has expressly created a power of interception, monitoring and decryption.^{xii} However, legality should not be reduced to the existence of a statute. A constitutional framework also requires that the law provide meaningful

standards against arbitrary executive action. A broad statutory power may become constitutionally problematic if its application is uncontrolled or unpredictable.

Section 69 requires the competent authority to be satisfied that interception is “necessary or expedient” for specified purposes and requires reasons to be recorded in writing. The requirement of written reasons is important because it creates a basis for subsequent review. It should not, however, be interpreted as a purely formal exercise.

The authority should identify the statutory ground relied upon and explain why the information sought is connected to that ground. In a criminal investigation, the reasons should indicate the nature of the offence and the investigative need. Where feasible, the order should identify the relevant person, account, device, computer resource or category of information.

The legality requirement also supports record keeping. A secret surveillance system must create a documentary trail sufficient for independent review. Without such records, it becomes difficult to determine whether officials acted within the limits of the law.

The constitutional objective is therefore structured discretion. Section 69 should be administered so that the existence of a statutory power does not become a presumption that every technologically available form of surveillance is legally permissible.

VI. LEGITIMATE STATE AIM AND INVESTIGATIVE NECESSITY

The purposes listed in Section 69 are, in general, legitimate governmental objectives. National security, defence, public order and criminal investigation are central functions of the State. Privacy cannot be interpreted as preventing the government from protecting individuals and the nation from serious threats.

The constitutional issue arises when a legitimate purpose is used to justify a measure that is broader than necessary. A legitimate end does not automatically validate every means adopted to achieve it.

The necessity requirement requires attention to alternatives. If investigators can obtain the relevant evidence through a narrowly targeted request,

unrestricted monitoring may be difficult to justify. Similarly, if information is already lawfully available from another source, an intrusive interception may not be necessary.

Necessity should be assessed in relation to the facts known at the time of authorisation. Authorities cannot be expected to predict the future with certainty, but they should be able to identify a rational investigative basis for believing that the surveillance will produce relevant information.

The seriousness of the alleged offence is also relevant. Intrusive surveillance may be easier to justify in relation to serious organised crime or credible national-security threats than in relation to minor offences. This does not mean that privacy disappears in serious cases; rather, the State interest is stronger and may justify a greater degree of intrusion if other requirements are satisfied.

The constitutional balance is therefore contextual. A rigid rule that either permits or prohibits surveillance in all cases would fail to account for differences in the nature of offences, evidence and privacy interests.

VII. PROPORTIONALITY AFTER PUTTASWAMY

Proportionality has become a central principle for examining restrictions on fundamental rights. The Supreme Court’s jurisprudence requires consideration of the relationship between the governmental objective and the rights-restricting measure, the availability of less restrictive alternatives and the overall balance between competing interests.^{xiii}

Applied to Section 69, proportionality requires at least four practical inquiries.

First, there must be a legitimate objective. Investigation of an offence or protection of national security may satisfy this requirement.

Second, there must be a rational connection between surveillance and that objective. Authorities should be able to explain why the particular digital information sought is expected to assist the investigation.

Third, surveillance should be necessary. Where less intrusive alternatives can reasonably achieve the same objective, the more intrusive measure should ordinarily not be preferred.

Fourth, the intrusion must be proportionate in its overall effect. Access to a year of personal

correspondence, for example, may be substantially more intrusive than interception of a single communication. The duration and breadth of surveillance therefore matter.

Proportionality should also operate at the implementation stage. An order may be lawful in principle but implemented in a manner that exceeds what was authorised. Filtering, access controls and restrictions on dissemination can help prevent such overreach.

The post-Puttaswamy approach thus changes the question from “Is surveillance authorised?” to “Is this particular surveillance justified?” That is a more demanding constitutional inquiry and is appropriate given the capacity of modern technology to penetrate personal life.

VIII. EXECUTIVE AUTHORISATION AND THE NEED FOR INDEPENDENT OVERSIGHT

One of the most important questions concerning Section 69 is whether executive authorisation, combined with existing review mechanisms, provides sufficient protection against arbitrary surveillance.

PUCL responded to the problem of executive surveillance by requiring procedural safeguards and review.^{xiv} The safeguards were developed in the context of telephone tapping under the Telegraph Act. Digital surveillance under Section 69 can be substantially broader because computer resources may contain a large variety of stored and transmitted information.

The concern is institutional rather than personal. An agency seeking surveillance may have a strong investigative interest in obtaining access. If the authorisation process is located entirely within the executive branch, there may be a risk that the need for investigation will receive greater weight than the privacy interest of the person who is not present to argue against surveillance.

One possible reform is prior judicial authorisation for highly intrusive surveillance. Another is a specialised independent surveillance authority or tribunal. Either model could provide a degree of institutional separation between the agency requesting access and the authority deciding whether access is justified.

Independent review should examine the seriousness of the alleged offence, the evidentiary basis, the

precise information sought, the duration, the expected investigative value and less intrusive alternatives.

The argument for independent scrutiny becomes stronger as the surveillance becomes more intrusive. It may be unnecessary to create a burdensome judicial process for every minor technical request, but access to extensive private communications should receive a correspondingly high level of scrutiny.

Such oversight would not weaken law enforcement. Properly designed oversight can strengthen the credibility and legal sustainability of investigative action.

IX. SECRECY, TRANSPARENCY AND REMEDIES

Surveillance necessarily involves secrecy. If a suspect is warned before an interception, the investigation may be frustrated. Therefore, immediate notice to the target cannot be treated as an absolute requirement.

Yet secrecy creates a constitutional accountability problem. A person who does not know that surveillance occurred may have little opportunity to challenge an unlawful intrusion. The State must therefore compensate for secrecy through institutional oversight, documentation and review.

Surveillance orders should contain reasons and should be subject to review. Records should identify the authorising authority, period of surveillance and information covered. Access to intercepted material should be restricted and auditable.

Aggregate transparency is also possible. Government can publish general statistics about the number of interception requests, broad categories of offences and review outcomes without revealing operational details. Such reporting would enable Parliament, courts and the public to understand how extensively the power is being used.

A further possibility is post-surveillance notification in cases where disclosure would no longer prejudice an investigation or legitimate national-security interest. The notification could enable individuals to seek a remedy where surveillance was unlawful.

Effective remedies are especially important because surveillance is invisible by nature. If a constitutional right can be violated without the affected person ever knowing, the system requires strong institutional

safeguards to prevent the right from becoming purely theoretical.

X. COLLATERAL SURVEILLANCE AND DATA MINIMISATION

Digital communications are relational. When authorities intercept the communications of one person, they may simultaneously collect information belonging to other people. This is collateral surveillance.

For example, an intercepted conversation may contain information concerning family members, colleagues, clients or friends. An email account may contain communications from persons who are not suspected of any offence. A digital device may contain photographs and documents belonging to several people.

This creates a difficult constitutional problem because third parties may have their privacy affected without any allegation against them.

Data minimisation provides one response. Authorities should collect and retain only information reasonably required for the authorised purpose. Irrelevant material should be filtered or destroyed where practicable.

Purpose limitation is equally important. Information collected for one criminal investigation should not automatically become a general-purpose database for unrelated governmental activities.

Retention must also be controlled. Digital information can be copied indefinitely, and the investigative justification for retaining material may disappear when an investigation ends or when information proves irrelevant.

A robust framework should therefore contain clear rules on storage periods, access controls, secure deletion and audit trails. These safeguards protect not only privacy but also the integrity of evidence. Excessive retention increases the risk of unauthorised disclosure, manipulation and misuse.

The constitutional right to privacy should consequently influence the entire information lifecycle: collection, access, analysis, sharing, retention and destruction.

XI. DECRYPTION AND ENCRYPTED COMMUNICATION

The inclusion of decryption in Section 69 creates a distinctive constitutional and technological issue. Encryption is widely used to protect personal communications, financial information, commercial data and professional confidentiality.

The State may have a legitimate need to obtain encrypted evidence in serious investigations. A narrowly tailored decryption direction concerning a specific account or communication may be capable of satisfying constitutional requirements when supported by proper authorisation.

A broader demand that weakens encryption for unrelated users is different. Systemic weakening of encryption can create security vulnerabilities that criminals and other unauthorised actors may exploit. The State interest in obtaining particular evidence must therefore be balanced against the security interest of millions of unrelated users.

The constitutional distinction should be between targeted access and generalised access. Targeted decryption can be linked to a specific investigative objective. A permanent or universal capability to bypass security is substantially harder to justify under necessity and proportionality.

Any technical assistance requirement should therefore be narrowly framed. Authorities should identify the information sought, explain its relevance and limit the demand to what is necessary.

The issue illustrates why post-Puttaswamy constitutional analysis cannot be separated from technological realities. A measure that appears limited from a purely legal perspective may have extensive consequences when implemented through modern digital systems.

XII. FREEDOM OF SPEECH AND CHILLING EFFECTS

Privacy and freedom of expression are interconnected. Individuals may change their lawful behaviour if they believe their private communications are being monitored. They may avoid controversial subjects, confidential discussions or communication with particular persons. Such a chilling effect can indirectly burden Article 19(1)(a).

The concern is especially serious for journalists, lawyers, researchers, whistle-blowers and other persons whose work depends upon confidential communication. Surveillance of a journalist's source, for example, can affect not only the journalist's privacy but also the broader public interest in receiving information.

This does not create an absolute immunity from lawful investigation. A journalist or lawyer may be investigated where the law permits it and where constitutional requirements are satisfied. However, the professional character of the communication may be relevant to proportionality and should be considered before access is authorised.

The safeguards surrounding privileged or sensitive communications should therefore be stronger. Where material unrelated to the suspected offence is incidentally collected, it should not automatically become available for unrelated purposes.

PUCL recognised that telephone tapping could affect freedom of speech as well as privacy.^{xv} The same constitutional logic becomes more important in the digital environment, where communications can be more extensive and revealing.

Section 69 should consequently be applied in a manner that recognises the chilling-effect dimension of surveillance and preserves legitimate spaces for confidential communication.

XIII. ARTICLE 14 AND ARBITRARY SURVEILLANCE

Article 14 provides additional constitutional control because arbitrary State action is inconsistent with equality before law and non-arbitrariness.

Surveillance decisions can become arbitrary if similarly situated cases are treated differently without rational justification or if officials exercise discretion without consistent standards. One authority may require substantial investigative material while another may rely on vague suspicion.

Written reasons, objective criteria and independent review can reduce this risk. Authorities should be able to explain why surveillance was considered necessary in a particular case and why the chosen scope and duration were appropriate.

Article 14 also reinforces the requirement of consistency. The existence of an offence does not itself create a licence for unlimited surveillance. The

nature and seriousness of the offence, the quality of the evidence and the intrusiveness of the proposed measure should influence the decision.

The relationship between Articles 14 and 21 is therefore important. A proportionality-based surveillance framework not only protects privacy but also disciplines administrative discretion. It ensures that intrusive powers are exercised according to reasons that can be examined rather than personal preference.

A constitutional system should not depend upon the assumption that officials will always act correctly. It should create institutional structures that make unlawful or arbitrary action more difficult and easier to detect.

XIV. CRITICAL ANALYSIS OF SECTION 69

Section 69 possesses significant legal strengths. It provides express statutory authority for interception, monitoring and decryption. It identifies governmental objectives and requires reasons to be recorded. The 2009 Rules add procedural safeguards. These features distinguish the provision from completely unregulated surveillance.

Nevertheless, the post-Puttaswamy framework reveals several areas requiring stronger protection.

First, statutory expressions such as "necessary or expedient" are broad. They require disciplined interpretation so that they do not become a general authorisation for surveillance.

Second, executive-centred authorisation raises concerns about institutional independence, particularly for highly intrusive access.

Third, secrecy can limit the practical ability of individuals to challenge surveillance.

Fourth, digital interception can result in extensive collateral collection involving innocent third parties.

Fifth, decryption directions may affect the security of persons beyond the investigation.

Sixth, retention and secondary use of information require clear limits.

These concerns should not be converted into the proposition that Section 69 is unconstitutional in every application. A more defensible approach is to read the statutory framework consistently with Articles 14, 19 and 21. Where a provision permits multiple interpretations, the interpretation that

provides stronger protection against arbitrary intrusion should be preferred.

The critical question is therefore not whether surveillance exists, but whether the surveillance power is controlled. A constitutional democracy may require secrecy in individual investigations, but it cannot accept secrecy without accountability.

XV. REFORMS AND THE WAY FORWARD

A rights-compatible surveillance framework should incorporate several reforms.

First, prior independent authorisation should be considered for highly intrusive interception and decryption. Judicial warrants or a specialised independent surveillance authority could provide a stronger institutional check.

Second, orders should contain detailed reasons. The authorising authority should identify the statutory ground, the information sought, the connection with the investigation and the expected duration.

Third, surveillance should be narrowly targeted. Where technically feasible, orders should identify particular persons, accounts, devices, resources or categories of information.

Fourth, strict time limits should apply. Continuation should require fresh justification.

Fifth, the necessity assessment should be documented. Authorities should consider whether less intrusive methods could reasonably achieve the investigative objective.

Sixth, data minimisation should be mandatory. Irrelevant information should be segregated, restricted or destroyed.

Seventh, retention periods should be clear. Information should not be retained indefinitely merely because it was lawfully obtained.

Eighth, independent review should be meaningful. Review bodies should have access to records and should be capable of identifying non-compliance.

Ninth, professional and privileged communications should receive heightened protection, subject to narrowly defined exceptions.

Tenth, aggregate transparency reports should be published periodically. Transparency need not reveal operational details; statistical reporting can provide democratic accountability.

Finally, decryption orders should avoid systemic weakening of encryption. The objective should be

targeted access to relevant evidence rather than creation of indiscriminate surveillance capability.

These reforms would not abolish Section 69. They would make its operation more consistent with the constitutional values identified in Puttaswamy.

XVI. CONCLUSION

Section 69 of the Information Technology Act occupies an important position in India's digital criminal justice framework. Modern criminal investigation cannot ignore electronic evidence, and the State has legitimate responsibilities concerning national security, public order and serious crime. Interception, monitoring and decryption may therefore be constitutionally permissible in appropriate circumstances.

The constitutional difficulty arises because digital surveillance can penetrate personal life more deeply than many traditional investigative techniques. A computer resource can contain years of private information, and access to it can affect persons who are not suspects. The constitutional framework must therefore be sensitive to the scale, duration and nature of digital intrusion.

Puttaswamy provides that framework. Privacy is a fundamental right, and restrictions must satisfy constitutional requirements. PUCI remains significant because it demonstrates that surveillance must be accompanied by procedural safeguards. The post-Puttaswamy proportionality approach requires the State to justify the particular intrusion rather than merely point to the existence of statutory power.

Section 69 should consequently be understood as a controlled investigative authority. Its legitimacy depends upon lawful authorisation, legitimate purpose, necessity, proportionality and safeguards against misuse. The more intrusive the surveillance, the stronger the justification and independent scrutiny should be.

The future of surveillance law in India should therefore move towards targeted rather than indiscriminate surveillance, independent rather than purely internal oversight, limited rather than indefinite retention, and accountable rather than invisible governmental power.

The essential constitutional principle is simple: the State may investigate crime and protect national security, but it must do so within the discipline of law

and fundamental rights. Privacy is not an obstacle to criminal justice. It is a constitutional boundary within which criminal justice must operate. Section 69 can remain a useful investigative provision, but its post-

Puttaswamy application must be shaped by dignity, autonomy, necessity, proportionality and accountability.

FOOTNOTES

-
- ⁱ Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
- ⁱⁱ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- ⁱⁱⁱ People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- ^{iv} Information Technology Act, No. 21 of 2000, § 69 (India).
- ^v Id. §§ 69A–69B.
- ^{vi} M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
- ^{vii} Kharak Singh v. State of U.P., AIR 1963 SC 1295.
- ^{viii} People's Union for Civil Liberties, (1997) 1 SCC 301.
- ^{ix} Id.
- ^x Justice K.S. Puttaswamy (Retd.), (2017) 10 SCC 1.
- ^{xi} Id.
- ^{xii} Information Technology Act, No. 21 of 2000, § 69 (India).
- ^{xiii} Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353; Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
- ^{xiv} People's Union for Civil Liberties, (1997) 1 SCC 301.
- ^{xv} Id.

SELECTED BIBLIOGRAPHY

- [1] Constitution of India.
- [2] Information Technology Act, No. 21 of 2000.
- [3] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
- [4] Digital Personal Data Protection Act, No. 22 of 2023.
- [5] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- [6] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- [7] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
- [8] Kharak Singh v. State of U.P., AIR 1963 SC 1295.
- [9] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
- [10] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.