IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE LEGAL ASPECTS OF ELECTRONIC MONITORING AND SURVEILLANCE IN CRIMINAL INVESTIGATION

AMAN KULSHRESTHA

RESEARCH SCHOLAR

DEPARTMENT OF LAW, LNCT UNIVERSITY, BHOPAL

DR.(PROF.) N.K. THAPAK

VC & RESEARCH GUIDE

DEPARTMENT OF LAW, LNCT UNIVERSITY, BHOPAL

ABSTRACT: Electronic monitoring and surveillance have become essential tools in modern criminal investigation because crimes increasingly involve digital communication, devices, and networks. At the same time, these tools raise serious legal questions about privacy, liberty, evidentiary fairness, and state power. This paper examines the legal framework governing electronic surveillance, focusing on Indian law with comparative references where useful, and argues that effective investigation must be balanced by clear authority, procedural safeguards, and meaningful oversight.

INDEX TERMS - Electronic monitoring, surveillance, CCTV-based tracking, GPS monitoring, metadata analysis, biometric identification, spyware, predictive policing algorithms

I. INTRODUCTION

Electronic monitoring and surveillance encompass the interception, observation, recording, and analysis of communications or digital activities for investigative purposes. In the realm of criminal law, these techniques may involve phone interception, message monitoring, access to computer data, tracking via CCTV, GPS monitoring, and the search or seizure of electronic devices. Their significance is clear: they assist investigators in identifying suspects, preserving evidence, and reconstructing events. Due to their intrusion into personal privacy, these methods must be legally justified and constrained by constitutional principles.

Electronic monitoring and surveillance have become essential tools in modern criminal investigations, driven by the rapid growth of digital technology, internet communication, and cyber-enabled crimes. In today's world, criminal activities extend beyond physical locations; they increasingly involve mobile phones, encrypted messaging apps, social media, electronic financial transactions, cloud storage, and interconnected

digital networks. Organized crime groups, cybercriminals, terrorists, money launderers, and even average offenders frequently utilize digital tools to plan, execute, and hide illegal activities. As a result, investigative agencies heavily depend on techniques such as phone tapping, interception of electronic communications, GPS tracking, CCTV surveillance, internet monitoring, metadata analysis, biometric identification, and data extraction from digital devices to detect and prevent crime, gather evidence, and uphold national security. The increasing reliance on electronic surveillance has fundamentally altered the landscape of criminal investigation. Traditional investigative methods, such as eyewitness accounts, physical searches, and confessions, are progressively being supplemented or replaced by digital evidence produced through surveillance technologies. Today, law enforcement agencies employ advanced software, artificial intelligence, and other technological innovations to enhance their investigative capabilities.

In India, the legal framework that governs electronic surveillance is fundamentally based on constitutional principles, statutory provisions, executive regulations, and judicial interpretations. The Constitution of India ensures the protection of life and personal liberty as stated in Article 21, which has been interpreted by the judiciary to encompass the right to privacy. Although privacy is not explicitly mentioned as a fundamental right in the Constitution, judicial rulings have increasingly acknowledged it as essential to human dignity and liberty. The legal discourse revolves around a classic conflict. On one hand, there is the state's obligation to prevent crime and ensure public safety; on the other hand, there is the individual's right to privacy and due process. In India, this conflict intensified following the acknowledgment of privacy as a fundamental right in the case of Justice K.S. Puttaswamy v. Union of India, as well as the introduction of new digital interception regulations. The landmark ruling by the Supreme Court in Justice K.S. Puttaswamy v. Union of India firmly established privacy as a constitutionally protected fundamental right under Article 21. The Court underscored that any infringement of privacy by the state must meet the criteria of legality, necessity, proportionality, and procedural safeguards. This ruling significantly transformed the legal conversation regarding electronic surveillance in India by mandating that the state justify surveillance actions within constitutional boundaries. Statutorily, electronic surveillance in India is regulated through several enactments. The Indian Telegraph Act, 1885 authorizes interception of telephone communications under specified circumstances such as public emergency or public safety. Section 5(2) of the Act empowers the government to intercept messages in the interests of sovereignty, integrity, security of the state, friendly relations with foreign states, public order, or prevention of incitement to offences. Similarly, the Information Technology Act, 2000 provides legal authority for interception, monitoring, and decryption of electronic information under Sections 69, 69A, and 69B. These provisions allow the government to direct agencies to monitor digital communications and block online content under certain conditions. The procedural framework for such interception is further elaborated through rules framed under these statutes, including safeguards relating to authorization and review procedures.

Despite the existence of statutory provisions, concerns persist regarding the adequacy of safeguards and oversight mechanisms in India. Critics argue that many surveillance laws were enacted before the digital revolution and therefore fail to adequately address modern technological realities such as mass surveillance, artificial intelligence, data aggregation, and cross-border digital communication. In many instances, surveillance orders are issued through executive authorization without prior judicial approval, raising questions regarding transparency, accountability, and protection against abuse. The absence of a comprehensive data protection framework for many years further intensified concerns about unauthorized access, retention, and misuse of personal data collected through surveillance activities.

Judicial intervention has thus been crucial in establishing protections against arbitrary surveillance. Indian courts have consistently highlighted that the powers of surveillance must not be exercised in an unrestricted or mechanical fashion. In the case of People's Union for Civil Liberties v. Union of India, the Supreme Court

established procedural safeguards for telephone interception, which include necessity, limited duration, record maintenance, and oversight committee reviews. The Court acknowledged that telephone conversations are a significant component of private life and that arbitrary interception would infringe upon constitutional protections. Subsequent judicial rulings have continued to assess the equilibrium between national security concerns and individual rights in light of technological progress. Comparatively, several democratic jurisdictions have developed more elaborate regulatory frameworks governing surveillance. Countries such as the United States, the United Kingdom, and members of the European Union have enacted detailed laws requiring judicial warrants, parliamentary oversight, independent review bodies, and data protection safeguards. International human rights instruments, including the United Nations framework on civil and political rights, also recognize privacy as a fundamental human right that must not be subjected to arbitrary interference. Comparative analysis demonstrates that while surveillance may be necessary for legitimate state objectives, democratic societies increasingly insist upon proportionality, transparency, accountability, and independent supervision to prevent abuse.

The rapid advancement of technology has further complicated the legal and ethical dimensions of surveillance. Emerging technologies such as facial recognition systems, biometric databases, spyware, predictive policing algorithms, drones, and artificial intelligence-based monitoring tools have significantly expanded the surveillance capacity of the state. These technologies can collect and analyze personal information on an unprecedented scale, creating the possibility of mass surveillance rather than targeted investigation. Such developments raise critical questions concerning informed consent, algorithmic bias, discrimination, data security, and the limits of state power in a constitutional democracy.

Against this background, the present study seeks to critically examine the constitutional and statutory framework governing electronic monitoring and surveillance in India. It analyzes the extent to which existing laws strike a balance between the legitimate needs of criminal investigation and the protection of individual rights. The study also evaluates judicial approaches toward privacy and surveillance, identifies gaps and challenges in the current legal regime, and considers comparative international practices that may guide legal reform. The central argument of this paper is that while electronic surveillance is an essential tool for effective law enforcement and national security, its exercise must remain subject to clear legal authority, procedural safeguards, judicial scrutiny, and democratic accountability. Without such safeguards, surveillance powers risk undermining the very constitutional values that the legal system seeks to protect. The challenge before modern legal systems is not whether surveillance should exist, but how it should be regulated in a manner consistent with constitutionalism, rule of law, and human rights. A balanced legal framework must ensure that investigative efficiency does not come at the cost of civil liberties, and that technological progress is accompanied by equally robust mechanisms for protecting privacy, dignity, and individual freedom.

II. OBJECTIVE OF STUDY

- To examine the legal framework governing electronic surveillance,
- To focus on Indian law with comparative references and examine the procedural safeguards, and meaningful oversight.

III. RESEARCH METHODOLOGY

The research design used in this study was qualitative, descriptive, and analytical design only based on the use of secondary data. This type of methodology is explained by the purpose of the research to examine the current legal frameworks, policy documents, and institutional frameworks and not to collect primary data in the field. In this study, solely the analysis of documentaries and literature has been made. Relevant secondary data will be acquired by way of the following- The Constitution of India, The Information Technology Act,

2000, Telecommunications Act, 2023, The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024

IV. MEANING AND FORMS

Electronic surveillance covers several investigative techniques. The most common are -

A. INTERCEPTION OF COMMUNICATIONS

Interception of communications refers to the act of secretly monitoring, accessing, recording, collecting, or acquiring private communications transmitted through various communication channels. Such communications may include telephone calls, emails, text messages, internet usage, social media interactions, video calls, electronic data transmissions, and other forms of digital communication. In criminal investigations and national security operations, interception is used by law enforcement and intelligence agencies to obtain information regarding criminal activities, prevent threats to public order, and gather evidence against offenders.

Traditionally, interception was limited to telephone tapping and postal surveillance, but technological advancement and digital communication systems have significantly expanded the scope of interception. Today, governments possess the capability to monitor communications through mobile networks, internet platforms, satellite systems, encrypted applications, and digital databases. As modern crimes increasingly involve electronic devices and online communication, interception has become one of the most powerful investigative tools available to the state. The primary objective of interception is to detect, prevent, investigate, and prosecute criminal activities. It is commonly employed in cases involving terrorism, organized crime, cybercrime, drug trafficking, espionage, money laundering, corruption, and threats to national security. Interception helps investigative agencies identify suspects, trace criminal networks, monitor conspiracies, and collect evidence that may otherwise remain inaccessible. In many cases, intercepted communications provide direct proof of criminal intent, planning, or participation in unlawful activities.

B. MONITORING OF STORED DATA

Monitoring of stored data refers to the process by which law enforcement agencies, intelligence authorities, or other governmental bodies access, examine, collect, preserve, or analyze electronic information that has already been stored in digital form. Unlike interception of communications, which involves the real-time monitoring of ongoing communication, monitoring of stored data concerns information that exists in electronic storage systems such as computers, mobile phones, servers, cloud platforms, databases, hard drives, emails, social media accounts, CCTV recordings, and other digital repositories. In the digital age, individuals and organizations generate enormous quantities of electronic data through everyday activities including communication, banking, online transactions, browsing, social networking, and use of digital devices. This stored information often becomes an important source of evidence in criminal investigations because it can reveal patterns of behavior, financial transactions, location history, communication records, photographs, videos, and other relevant material. As a result, monitoring of stored data has become an essential component of modern policing and criminal justice administration.

The primary objective of monitoring stored data is to obtain evidence relating to criminal activity, identify suspects, reconstruct events, trace digital footprints, and prevent threats to public order or national security. Investigative agencies commonly access stored data in cases involving cybercrime, terrorism, corruption, money laundering, financial fraud, child exploitation, organized crime, narcotics trafficking, and digital offences. Electronic records frequently provide reliable and objective evidence because digital devices

automatically record information such as timestamps, location details, user activity, and communication history.

Stored data may exist in various forms. It includes:

- Emails saved on servers,
- Chat histories and social media messages,
- Call detail records,
- Cloud storage files,
- Browsing history,
- CCTV footage,
- Biometric information,
- Banking and financial records,
- Metadata,
- GPS and location records,
- Digital photographs and videos,
- Deleted or encrypted files recoverable through forensic tools.

Monitoring of stored data also includes forensic examination of digital devices such as laptops, smartphones, tablets, pen drives, and external hard drives. Digital forensic experts use specialized techniques to recover deleted files, analyze encrypted data, trace internet activity, and establish links between suspects and criminal activities. Consequently, digital evidence has become increasingly significant in judicial proceedings.

C. DECRYPTION OF COMPUTER RESOURCES

Decryption of computer resources refers to the process of converting encrypted or coded digital information into a readable and accessible form through the use of cryptographic keys, software tools, or technical mechanisms. Encryption is a security technique used to protect electronic data, communications, and digital systems from unauthorized access. It transforms readable information, known as plaintext, into an unreadable format called ciphertext. Decryption is therefore the reverse process through which encrypted information is decoded so that it can be understood or used by authorized persons. In the contemporary digital era, encryption has become an essential component of cybersecurity and data protection. Individuals, corporations, financial institutions, government agencies, and communication platforms widely use encryption to secure emails, online banking transactions, cloud storage, social media communication, passwords, and confidential information. Technologies such as end-to-end encryption, virtual private networks (VPNs), secure messaging applications, and encrypted databases are designed to protect user privacy and prevent unauthorized surveillance, hacking, or data theft.

D. DEVICE-BASED SEARCHES OR TRACKING

Device-based searches or tracking refer to investigative techniques through which law enforcement agencies or governmental authorities access, monitor, examine, or trace electronic devices and their associated digital information for the purpose of criminal investigation, intelligence gathering, or national security operations. These measures generally involve the use of technological tools to identify the location, activities, communication patterns, or stored data of a person through electronic devices such as mobile phones, laptops, tablets, GPS systems, smart watches, vehicles, and other internet-connected devices.

In the digital era, electronic devices have become an integral part of daily life. Individuals routinely use smartphones, computers, and digital applications for communication, banking, transportation, social networking, professional activities, and storage of personal information. These devices continuously generate and store large amounts of data relating to location, movement, contacts, browsing history, transactions, photographs, biometric information, and communication records. Consequently, device-based searches and tracking have become extremely important tools for modern criminal investigation because digital devices often contain critical evidence relating to criminal conduct.

Device-based searches generally involve direct examination or extraction of information from an electronic device. Investigative authorities may seize devices during searches, inspect digital contents, recover deleted files, analyze communication history, or conduct forensic examinations using specialized software tools. Such searches may reveal evidence regarding criminal planning, financial transactions, online activities, associations between suspects, or possession of unlawful material.

Tracking, on the other hand, involves monitoring the physical location or movement of an individual or object through technological means. Tracking technologies commonly include:

- Global Positioning System (GPS) devices,
- Cell-site location information (CSLI),
- Mobile tower triangulation,
- Bluetooth and Wi-Fi tracking,
- Radio-frequency identification (RFID),
- Vehicle tracking systems,
- Geolocation data generated by mobile applications,
- Biometric surveillance,
- Internet-connected smart devices.

Law enforcement agencies frequently use these technologies to trace suspects, reconstruct movements, identify crime scenes, monitor travel patterns, and prevent unlawful activities.

Device-based searches and tracking are widely used in investigations relating to terrorism, cybercrime, kidnapping, organized crime, narcotics trafficking, financial fraud, human trafficking, and national security threats. Mobile phones and digital devices often provide direct evidence regarding communication between accused persons, participation in criminal conspiracies, or location at the time of commission of offences. GPS tracking and geolocation analysis also assist authorities in identifying routes, movement patterns, and connections between suspects. In practice, these techniques are used for both preventive and reactive investigation, especially in terrorism, organized crime, cybercrime, financial fraud, narcotics, and corruption cases. Electronic monitoring is slightly different from surveillance in the narrow sense. It often refers to tracking a person's location or compliance with legal conditions, such as bail or probation, using GPS devices or similar technology. Although it can reduce prison populations and improve supervision, it still involves collection of highly sensitive location data and therefore raises privacy and proportionality concerns. For research purposes, it is useful to separate investigatory surveillance from post-charge or correctional monitoring, because the legal standards and policy goals are not identical.

V. INDIAN LEGAL FRAMEWORK

Indian law has historically relied on a fragmented framework rather than one comprehensive surveillance statute. Section 69 of the Information Technology Act, 2000 empowers the government to intercept, monitor,

and decrypt information stored in a computer resource for purposes connected with public safety and public order. In the telecommunications context, the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, notified under the Telecommunications Act, 2023, now govern interception of messages and replace the older interception regime under the Indian Telegraph Rules.

The current Indian framework emphasizes authorization and procedural control. The 2024 rules, as summarized in legal reporting, allow interception only when necessary information cannot reasonably be obtained by other means, require competent-authority approval, limit orders to a defined duration, and create review mechanisms for compliance. These features are important because they show an attempt to move from broad executive discretion toward structured legal oversight. At the same time, commentary on India's surveillance regime continues to describe it as fragmented and in need of a dedicated statute, especially after the DPDP Act and the new criminal laws.

VI. CONSTITUTIONAL LIMITS

The constitutional issue is whether surveillance satisfies the requirements of legality, necessity, and proportionality. After Justice K.S. Puttaswamy Vs. Union Of India (2017) 10 SCC 1, privacy is no longer treated as a weak interest; it is a constitutionally protected right under Article 21, and surveillance measures must be justified against that standard. That means a law authorizing surveillance must be clear, non-arbitrary, and supported by safeguards against abuse.

The requirement of legality implies that surveillance must be backed by a valid law that is clear, accessible, and not vague. Arbitrary executive action without statutory backing would violate Article 14 (Right to Equality), which prohibits arbitrariness in state action. Thus, any surveillance law must ensure non-discriminatory application and provide procedural safeguards. The principle of necessity requires that surveillance should only be undertaken for a legitimate state aim, such as national security, public order, or prevention of crime. This connects with reasonable restrictions permitted under Article 19(2) on the freedom of speech and expression (Article 19(1)(a)). However, such restrictions must not be excessive or disproportionate to the objective sought to be achieved.

The doctrine of proportionality further ensures that even if surveillance serves a legitimate aim, the method adopted must be the least intrusive measure available. Indiscriminate or mass surveillance, without adequate justification, would fail this test as it disproportionately infringes individual freedoms.

A second major concern relates to freedom of speech and expression under Article 19(1)(a). Excessive or unchecked surveillance can create a "chilling effect", where individuals refrain from expressing opinions, engaging in political dissent, or practicing journalism due to fear of being monitored. This undermines democratic values and weakens public participation. Confidential communications, including lawyer-client or journalist-source interactions, are particularly vulnerable.

A third issue is due process and procedural fairness, rooted in Articles 21 and 14. If surveillance powers are exercised solely by the executive without independent judicial or parliamentary oversight, the risk of abuse significantly increases. The absence of safeguards such as prior judicial approval, periodic review, and accountability mechanisms can lead to misuse for political or personal purposes.

Article 20(3) (protection against self-incrimination) may also be implicated where surveillance compels individuals to disclose personal data or communications that could be used against them. Similarly, Article 22 (protection against arbitrary arrest and detention) becomes relevant where surveillance leads to coercive state action without proper safeguards.

In sum, constitutional scrutiny of surveillance in India requires a careful balance between state interests (security, order) and individual rights (privacy, liberty, free speech). Any surveillance framework must therefore be grounded in clear law, pursue a legitimate aim, adopt proportionate means, and incorporate strong institutional safeguards to prevent abuse.

VII. INVESTIGATION AND EVIDENCE

Electronic surveillance is most valuable when it produces reliable evidence that can be used in court. But legality and admissibility are not the same thing. A major question in Indian criminal procedure is whether unlawfully obtained electronic evidence should be excluded; scholarship notes that Indian courts have historically focused on relevance rather than on a strong exclusionary rule. That creates an incentive problem: even illegal surveillance may still produce evidence that is later admitted.

Search and seizure of electronic devices is another unresolved area. A 2024 study found that India still lacks a dedicated law regulating search and seizure of electronic devices in criminal investigation, although Virendra Khanna v. State of Karnataka (2021 SCC OnLine Kar 1332) provided some guidance. This gap matters because devices contain far more than the evidence needed for a single case; they can reveal messages, contacts, location history, photos, passwords, and intimate personal records. For this reason, courts and investigators must think carefully about scope, device cloning, hash values, chain of custody, and minimization of irrelevant data.

VIII. SAFEGUARDS

The legitimacy of surveillance depends on safeguards. The first safeguard is prior authorization by a legally competent authority, because unchecked executive access invites abuse. The second is necessity: interception should be permitted only when less intrusive methods are insufficient. The third is proportionality: the scope and duration of surveillance should be tied tightly to the seriousness of the offense and the investigative need.

Oversight is equally important. Review committees, periodic renewal, record destruction rules, and confidentiality obligations help reduce the risk of long-term misuse. Transparency is also important at the systemic level, even if individual surveillance orders cannot always be disclosed during an investigation. Without transparency, it becomes difficult to assess whether surveillance powers are being used for serious crime control or for routine overreach.

The Case For Practical Necessity

- **Investigating Complex Conspiracies:** Organized crime syndicates and terrorist networks rely heavily on secure, decentralized communication. Intercepting these channels is often the only way law enforcement can map out the hierarchy of a conspiracy and intervene before a crime occurs.
- **Decoding Cyber offenses:** Cross-border cyber offenses and financial crimes heavily obscure the identities of perpetrators. Electronic monitoring tools like IP tracking and digital forensics are crucial for tracing illegal transactions, seizing assets, and prosecuting hackers.
- **Preserving Admissible Proof:** Data like metadata, location history, and encrypted message fragments frequently constitute the "smoking gun" in a trial. Without electronic monitoring, these critical trails of digital evidence would remain inaccessible, allowing offenders to evade justice.
- **The Danger of Power Creep**- The "Scope Creep" Phenomenon- State surveillance powers inherently tend to expand past their original intent. Powers originally justified for combating severe threats like

terrorism often end up being used for general observation, routine policing, or monitoring activists and journalists.

- **Erosion of Privacy:** Without strict boundaries, the mass collection of metadata, location data, and communication logs severely infringes on personal privacy. This pervasive tracking can also create a "chilling effect," where citizens censor their own speech, associations, and online activities out of fear of state observation.

IX. COMPARATIVE PERSPECTIVE

Comparative law helps show where India stands. In the United States, electronic surveillance is typically framed by warrant requirements, judicial approval, and constitutional exclusionary rules, which makes unlawful interception easier to challenge. That model does not eliminate surveillance abuse, but it places stronger limits on executive discretion.

India, by contrast, has moved toward more detailed interception rules, especially in the telecom sector, but still lacks a single comprehensive surveillance statute that clearly defines powers, procedures, oversight, retention, and remedies across all technologies. This fragmentation is a recurring theme in legal scholarship. A dedicated statute could unify standards for interception, device searches, metadata access, retention periods, and remedies for unlawful surveillance.

X. CRITICAL EVALUATION

The strongest argument in favor of surveillance is practical necessity. Digital evidence often provides the only reliable proof in complex conspiracies, encrypted communications, and cross-border cyber offenses. Without electronic monitoring, many modern crimes would be far harder to detect and prosecute.

The strongest argument against surveillance is that power tends to expand beyond its original justification. Once the state can monitor messages, devices, and movements, weak safeguards can quickly turn targeted investigation into generalized observation. The legal challenge is not to eliminate surveillance, but to ensure that it remains targeted, reviewable, and proportionate. That requires clear law, independent oversight, and remedies that matter in court. Surveillance represents a fundamental tension between maintaining public safety and protecting individual civil liberties. It requires a continuous, delicate balance between practical enforcement needs and democratic freedoms.

XI. THE PATH FORWARD: TARGETED, PROPORTIONAL SAFEGUARDS

- **Clear Legal Frameworks:** Surveillance frameworks must be strictly codified to define what can be intercepted, under what conditions, and for how long - Clear legal frameworks are essential to ensure that surveillance activities are conducted lawfully, transparently, and with respect for individual rights. Such frameworks should clearly specify the types of communications, data, or activities that may be intercepted, the legitimate purposes for which surveillance can be authorized (such as national security or criminal investigations), and the authorities responsible for approving and overseeing these actions. They should also establish strict conditions for obtaining warrants or authorization, define the duration for which surveillance can be carried out, and set limits on the collection, storage, use, and sharing of intercepted information. By providing precise rules and safeguards, clear legal frameworks help prevent abuse of power, protect citizens' privacy, and ensure that surveillance measures remain proportionate, accountable, and subject to judicial or independent oversight.
- **Independent Oversight:** Authorizing surveillance cannot rely solely on the executive branch or secret police processes. Intercepting private data requires warrants or authorization from independent judicial

bodies to ensure investigations remain tightly targeted. Independent oversight is a fundamental safeguard in any surveillance system because it helps prevent the misuse of government power and protects citizens' civil liberties. Decisions to conduct surveillance should not be left solely to executive agencies, law enforcement bodies, or intelligence services, as this can create risks of bias, overreach, or politically motivated monitoring. Instead, requests to intercept private communications or access personal data should be reviewed and authorized by independent judicial authorities or other impartial oversight bodies. These institutions assess whether the surveillance request is supported by sufficient evidence, serves a legitimate purpose, and is proportionate to the threat or investigation involved. By requiring warrants or formal authorization, independent oversight ensures that surveillance activities remain narrowly focused, legally justified, and accountable, reducing the likelihood of unnecessary intrusions into individuals' privacy while maintaining public trust in security and law enforcement operations.

- **Judicial Recourse:** Citizens who are monitored unlawfully must have actionable remedies in court, which requires transparency mechanisms like regular disclosures of surveillance statistics

XII. CONCLUSION

Electronic monitoring and surveillance are now indispensable in criminal investigation, but they sit at the intersection of policing, privacy, and constitutional law. Indian law provides authority for interception and monitoring, yet the overall framework remains fragmented and still needs stronger coherence, especially for device searches, judicial oversight, and exclusion of illegally obtained evidence. The expansion of surveillance powers has simultaneously generated significant constitutional, legal, and ethical concerns. Electronic surveillance directly affects fundamental rights, particularly the right to privacy, personal liberty, freedom of speech and expression, and protection against arbitrary state action. Unlike conventional investigative techniques, digital surveillance allows the state to collect vast quantities of personal information, often without the knowledge or consent of individuals. Such surveillance may include monitoring private conversations, tracking locations, accessing emails and social media communications, and collecting sensitive personal data. The possibility of excessive or unchecked surveillance raises fears of misuse of power, political targeting, unlawful profiling, chilling effects on free expression, and erosion of democratic freedoms. The future of lawful surveillance in criminal justice should therefore be built on legality, necessity, proportionality, accountability, and respect for fundamental rights.

REFERENCES

1. The Constitution of India
2. Section 69 of the Information Technology Act, 2000
3. Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024,
4. Telecommunications Act, 2023
5. Overview of Electronic Surveillance in the United States: Law, Policy, and Practice. https://www.ojp.gov
6. The Status of Electronic Surveillance Laws in India: An Overview. https://techlawforum.nalsar

7. Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 commentary. www.visionias.com
8. Search and seizure of electronic devices in India: time for a change? www.journals.sagepub.com
9. The Surveillance State: Privacy and Criminal Investigation in India. https://papers.ssrn.com
10. Digital surveillance and Indian privacy laws. https://lijdlr.com