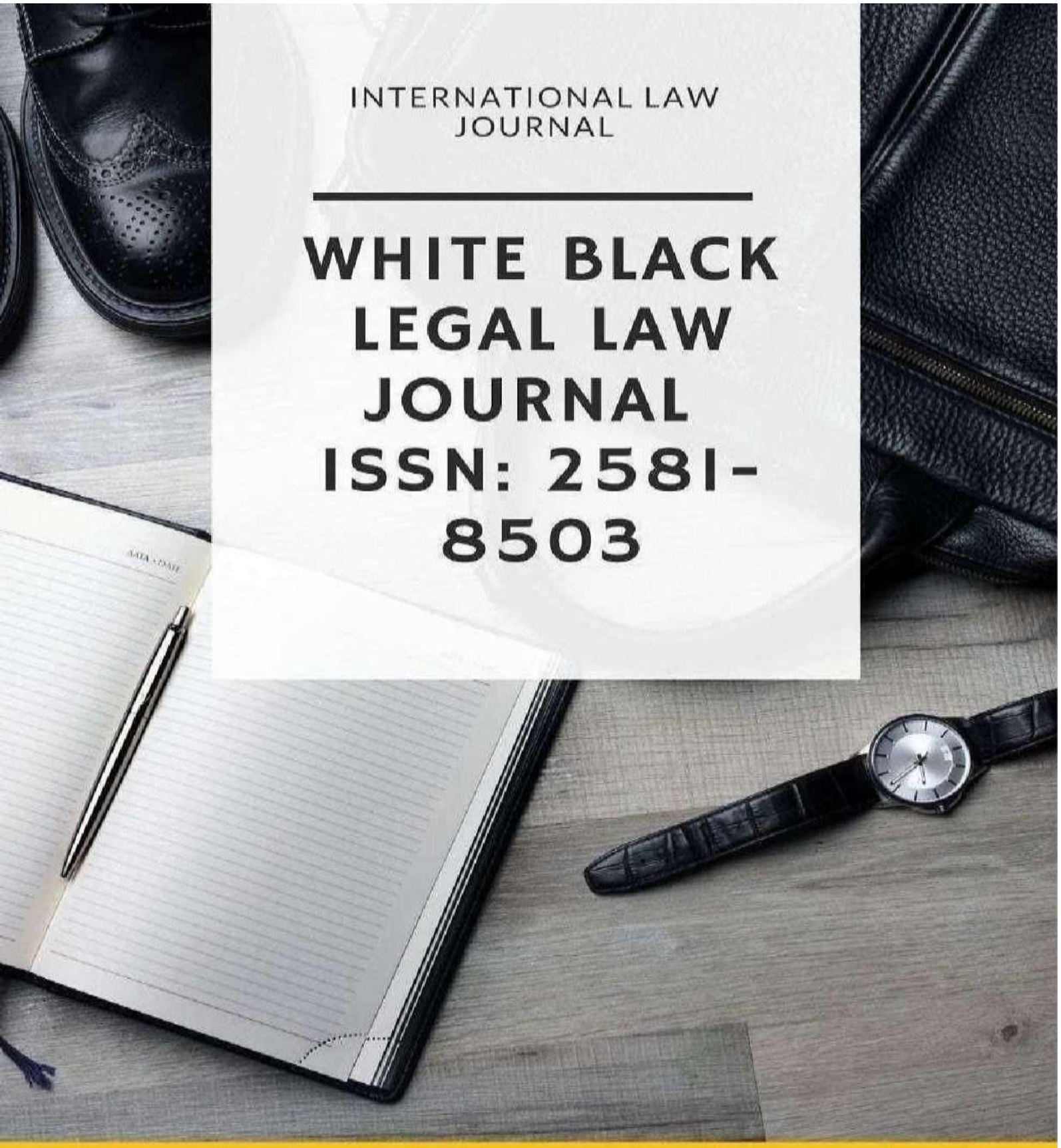

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

BALANCING NATIONAL SECURITY AND INDIVIDUAL RIGHTS: THE CONSTITUTIONAL VALIDITY OF DIGITAL SURVEILLANCE AND THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIA

AUTHORED BY - E. RANI
Assistant professor
Bharath Institute of Law.
173, Agaram Main Road, Selaiyur, Chennai.

The Legal Framework Governing Digital Surveillance in India

India's democratic fabric is deeply rooted in the Constitution, which guarantees its citizens fundamental rights essential for safeguarding personal autonomy and dignity. Among these, Articles 19(1)(a), 21, and 23 hold paramount significance as they protect the freedoms of speech and expression, personal liberty, and prohibit forced labor, respectively. Over time, the interpretation of these rights has expanded to include the right to privacy as an intrinsic facet of personal liberty under Article 21, thereby laying the foundation for the legal discourse surrounding digital surveillance. This interplay between individual rights and state powers to conduct surveillance, especially for national security, has fostered a complex legal environment that continues to evolve amidst rapid technological changes.

Article 19(1)(a) guarantees citizens the right to freedom of speech and expression, a cornerstone for a vibrant democracy. However, this right is not absolute and can be restricted by the state on grounds such as sovereignty, security of the state, public order, decency, or morality under Article 19(2). Personal liberty under Article 21 states that no person shall be deprived of life or personal liberty except according to procedure established by law. While Article 23 specifically prohibits trafficking and forced labor, its relevance to surveillance is indirect but underscores the state's obligation to uphold dignity and freedom. At the same time, Articles 69 and 70 of the Constitution empower the government to protect the sovereignty and integrity of India and maintain public order, granting it authority to conduct surveillance for national security and law enforcement.

The legal framework governing digital surveillance in India is a layered construct, comprising several statutory enactments, rules, and guidelines. The oldest and most prominent legislation in this realm is the Indian Telegraph Act, 1885. This act, though predating the digital era, provides the government the authority to intercept communications, including telephone and telegraph lines, under certain circumstances. Section 5(2) of the Indian Telegraph Act authorizes the government to order interception of messages in the interest of public safety, sovereignty, or to prevent incitement to an offense. However, the Act lacks specific provisions addressing the nuances of contemporary digital communication and data privacy, thereby rendering it somewhat archaic in the context of modern surveillance technologies.

Complementing the Telegraph Act is the Information Technology Act, 2000, which primarily deals with electronic governance, digital signatures, and cybercrimes but also contains provisions relevant to digital surveillance. For instance, Section 69 of the IT Act empowers the government to intercept, monitor, or decrypt any information generated, transmitted, or stored in any computer resource, again for reasons including national security and public order. This provision is supported by the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009, which lay down procedures for such surveillance to ensure some degree of transparency and accountability. Despite these procedural safeguards, the IT Act's scope for surveillance has drawn criticism for its broad and vague terms that may allow potential misuse or overreach by the state.

Beyond statutes, the Indian government has also issued various policy guidelines to strengthen cybersecurity and regulate digital data handling. Among these are the CERT In (Indian Computer Emergency Response Team) Guidelines, which mandate certain security practices and incident reporting obligations on digital service providers and network operators. While these guidelines play a crucial role in enhancing national cybersecurity resilience, their direct legal enforceability is limited. Moreover, the alignment of such guidelines with constitutional guarantees of privacy and freedom remains contentious, especially since they lack explicit judicial oversight mechanisms and clear limits on government access to personal data.

This legal framework, while comprehensive on paper, must be understood in the context of evolving jurisprudence that has shaped the balance between individual privacy rights and state interests. The landmark Supreme Court judgment in Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017) was a turning point in this discourse. In a unanimous decision, the Court

declared the right to privacy to be a fundamental right intrinsic to the freedoms guaranteed by the Constitution. This verdict transformed privacy from a mere legal principle into a justiciable constitutional right, thereby imposing stringent conditions on any state action that seeks to infringe upon privacy.

The Puttaswamy judgment emphasized that any intrusion on privacy must meet the criteria of legality, necessity, and proportionality. This means that surveillance programs or digital interceptions must be backed by clear legal authority, serve a legitimate aim such as national security or public safety, and be proportionate to the objective pursued. The Court further underscored the indispensability of judicial oversight to prevent arbitrary or excessive use of surveillance powers. This judgment led to the recognition that mass or bulk data collection without adequate safeguards would be unconstitutional, urging are examination of existing surveillance laws and practices.

Subsequent judicial pronouncements have reinforced the Puttaswamy principles by stressing due process and transparency in digital surveillance. Courts have reiterated that citizens must have access to effective remedies against unlawful surveillance and that any infringement must be procedurally justifiable, with adequate safeguards against abuse. This is particularly significant in cases involving digital footprints, which encompass a vast array of personal information such as internet browsing habits, location data, communication metadata, and social media activity. The courts have recognized that such data, if collected or monitored indiscriminately, can cause profound harm to individual autonomy, reputation, and democratic freedoms.

However, the legal landscape still faces challenges. The existing laws, notably the Indian Telegraph Act and the IT Act, have been criticized for lacking clear definitions of terms such as “interception,” “monitoring,” and “decryption,” creating ambiguity about the extent and limits of state surveillance. The procedural safeguards are often inadequate or not uniformly enforced, leading to concerns over arbitrary surveillance and inadequate accountability. Additionally, the absence of a comprehensive data protection law in India exacerbates these concerns, leaving personal data vulnerable to misuse without a clear statutory framework for consent, data minimization, and breach notifications.

In recent years, the Indian government has attempted to bridge this gap through various policy

initiatives and proposals for a dedicated data protection legislation. The Personal Data Protection Bill, which draws inspiration from the European Union's GDPR (General Data Protection Regulation), aims to establish robust frameworks for data privacy, including explicit consent requirements, rights to access and correction, and strict conditions for government access to personal data. Although this Bill is yet to be enacted, it signals a growing recognition of the need to balance state security concerns with individual privacy rights in the digital age.

Furthermore, the debate on surveillance has been influenced by technological advancements such as artificial intelligence, facial recognition, and mass data analytics, which enable unprecedented capabilities for monitoring and profiling individuals. These developments necessitate continuous judicial and legislative vigilance to ensure that surveillance does not morph into a tool for unwarranted state intrusion or social control. The courts, civil society, and lawmakers are increasingly aware that protecting digital privacy is crucial not only for individual freedoms but also for maintaining public trust and democratic legitimacy in an era dominated by digital communication. The legal framework governing digital surveillance in India is an intricate interplay of constitutional rights, statutory enactments, policy guidelines, and judicial pronouncements. While the Constitution provides the foundational guarantees of freedom, personal liberty, and privacy, laws like the Indian Telegraph Act and the Information Technology Act empower the state to conduct surveillance for legitimate purposes. The landmark Supreme Court judgment in Justice K.S. Puttaswamy has crystallized privacy as a fundamental right, mandating that surveillance must be necessary, proportionate, and subject to judicial oversight. Nevertheless, significant challenges persist in the form of outdated laws, inadequate safeguards, and rapid technological changes. India's journey towards a comprehensive and balanced digital surveillance framework continues, necessitating reforms that respect constitutional freedoms while addressing the imperatives of national security in a digital world.

Constitutional Challenges to Digital Surveillance in India

Digital surveillance is increasingly becoming a critical tool for governments worldwide to maintain national security, enforce law and order, and combat cybercrimes. However, in a democratic society like India, where the Constitution guarantees fundamental rights such as freedom of speech, expression, and privacy, the expanding scope of government surveillance has raised profound constitutional challenges. These challenges revolve around the potential of

surveillance to infringe on core civil liberties, disturb the delicate balance between state power and individual freedoms, and undermine democratic processes if not regulated with adequate safeguards and transparency.

At the heart of these concerns lies the constitutional right to privacy, which the Supreme Court of India unequivocally recognized as a fundamental right in the landmark 2017 judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India . Privacy is no longer a peripheral legal concept but a vital element intrinsic to the right to life and personal liberty under Article 21 of the Indian Constitution. Privacy encompasses not only physical solitude but also the control over one's personal data and communications in the digital sphere. Digital surveillance, if conducted without clear legal frameworks and oversight, risks breaching this right by enabling unwarranted intrusions into individuals' digital lives.

One of the major constitutional challenges posed by digital surveillance is its chilling effect on free speech and expression, guaranteed under Article 19(1) (a). When citizens are aware or even suspect that their communications, internet activities, or social media interactions are being monitored, they may self censor to avoid attracting government attention or retaliation. This "chilling effect" stifles open discourse, dissent, and democratic participation, which are essential for a healthy democracy. The Supreme Court, in various decisions, has underscored the need to protect these freedoms from undue state interference. Civil liberties organizations and activists have been at the forefront of raising alarms about the unchecked expansion of surveillance powers. They argue that the existing legal framework in India suffers from a lack of adequate procedural safeguards and transparency, which opens the door to misuse and abuse. One key demand is the establishment of an independent oversight mechanism, akin to a surveillance or data protection authority, tasked with ensuring that surveillance activities comply with constitutional standards and respect citizens' rights. Judicial pre authorization for interception and surveillance orders is also advocated as a critical safeguard to prevent arbitrary or excessive surveillance.

Currently, the Indian Telegraph Act, 1885, and the Information Technology Act, 2000, form the backbone of legal authority for digital surveillance. The Telegraph Act's provisions on interception date back to a pre digital era and lack nuanced regulation on new forms of electronic communication. The IT Act, while addressing digital communication, employs broad and vaguely worded powers under Section 69, which critics contend enable extensive

government intrusion without sufficient procedural checks or transparency. The procedural rules accompanying these laws, such as the Information Technology (Interception, Monitoring, and Decryption) Rules, 2009, fall short of international standards on independent oversight and clear limits on government powers. In light of these concerns, legal reforms have become imperative. Reform advocates argue that any legislation permitting surveillance must explicitly define its scope, establish strict necessity and proportionality tests, require prior judicial approval, and mandate transparency in reporting surveillance activities. Such reforms would align India's laws with the constitutional guarantee of privacy, ensuring that surveillance powers are exercised only to the extent necessary and justified by legitimate state interests like national security or crime prevention.

Comparative perspectives from other democratic jurisdictions offer valuable lessons for India's legislative and judicial efforts. The European Union's General Data Protection Regulation (GDPR) exemplifies a robust data protection regime that prioritizes individual consent, data minimization, and accountability of data controllers, including governmental agencies. Although GDPR primarily addresses data protection rather than surveillance per se, its principles set a global benchmark for privacy rights. The GDPR also requires transparency and grants individuals significant rights over their personal data, empowering citizens to challenge improper use or processing. In the United Kingdom, the Investigatory Powers Act, 2016—often dubbed the "Snooper's Charter"—regulates government surveillance powers with a framework emphasizing judicial oversight, independent commissioners, and clear authorization processes. Despite criticism for certain provisions, the Act requires surveillance activities to be authorized by senior officials and approved by judicial commissioners, establishing multiple layers of accountability. Importantly, the UK framework includes detailed record keeping and reporting obligations to Parliament and the public, helping to prevent abuse of powers. India's judiciary has increasingly echoed the need for such checks, balances, and transparency in digital surveillance. In the Puttaswamy judgment itself, the Supreme Court highlighted that the government must put in place clear, accessible, and effective legal safeguards to protect privacy and prevent misuse of surveillance technologies. Subsequent cases have reiterated that state action infringing on privacy must be strictly necessary, proportionate, and subject to independent judicial scrutiny. Courts have been wary of blanket or mass surveillance programs lacking individual suspicion or judicial authorization, warning that such programs threaten constitutional freedoms and democratic accountability.

Despite this progressive judicial stance, the Indian government has yet to enact a

comprehensive data protection and surveillance law that adequately addresses these constitutional challenges. The Personal Data Protection Bill, modeled on GDPR principles, has been proposed but is still under consideration and debate. Its enactment would represent a major step toward establishing clear rules on data privacy, government access to personal data, consent, and independent oversight. Until then, the absence of a modern statutory framework leaves India vulnerable to constitutional challenges and criticisms about government overreach in digital surveillance. Furthermore, technological advances present additional constitutional challenges. The deployment of mass data collection, facial recognition, biometric databases (such as Aadhaar), and AI based surveillance systems heightens the risks of arbitrary or discriminatory monitoring. Without robust legal safeguards, these technologies may infringe on privacy, facilitate profiling, and erode public trust in government institutions. The constitutional promise of equality under Article 14 is also at stake if surveillance disproportionately targets marginalized or dissenting groups. The constitutional challenges to digital surveillance in India are multifaceted and demand urgent attention. While the state has legitimate interests in ensuring national security and law enforcement, these must be balanced against fundamental rights to privacy, free speech, and personal liberty. Judicial pronouncements, especially the Puttaswamy judgment, have laid a solid foundation for protecting privacy rights and requiring surveillance to be necessary, proportionate, and subject to judicial oversight. Nonetheless, India's existing legal framework remains inadequate, necessitating comprehensive reforms inspired by global best practices. Establishing independent oversight bodies, mandating judicial pre authorization, enhancing transparency, and enacting a modern data protection law will be essential to safeguard democratic freedoms in the digital age. Only by embedding constitutional principles deeply into surveillance laws and practices can India ensure that digital surveillance serves the public interest without compromising the very rights that define its democracy.

The Admissibility of Electronic Evidence in Indian Courts

In an era dominated by digital communication and electronic transactions, courts worldwide face the challenge of accommodating digital evidence within traditional evidentiary frameworks. India, with its rapidly growing digital footprint, is no exception. The Indian legal system has progressively adapted to technological changes by integrating electronic evidence into its judicial processes. However, the admissibility of electronic evidence in Indian courts requires strict compliance with statutory provisions and judicial standards to ensure that such

evidence is reliable, authentic, and free from tampering.

Legal Framework Governing Electronic Evidence

The Indian Evidence Act, 1872, originally crafted in the pre digital era, was not designed to handle electronic evidence. Recognizing this gap, the legislature amended the Act in 2000 through the Information Technology Act, 2000 (IT Act), which introduced specific provisions addressing the admissibility of electronic records. Section 65B of the Indian Evidence Act, introduced by the IT Act, is the cornerstone for the admissibility of electronic evidence. This section stipulates that any information contained in an electronic record, when produced as evidence, must be accompanied by a certificate signed by a person occupying a responsible official position in relation to the operation of the relevant device. The certificate must affirm the manner in which the electronic record was produced, the integrity of the record, and compliance with prescribed procedures.

The essence of Section 65B is to establish a formal, objective assurance that electronic evidence has not been altered or tampered with, thus maintaining its integrity. This statutory requirement reflects an understanding of the technical vulnerabilities of digital data, which can be easily modified or fabricated.

Judicial Interpretation: Anvar P.V. v. P.K. Basheer

The Supreme Court's landmark judgment in Anvar P.V. v. P.K. Basheer (2014) marked a critical turning point in the jurisprudence of electronic evidence in India. In this case, the Court clarified and emphasized the mandatory requirement of producing a Section 65B certificate for the admissibility of electronic evidence.

Before Anvar, Indian courts were somewhat inconsistent in admitting electronic evidence, often relying on general principles of authenticity and relevance. However, the Supreme Court unequivocally held that any electronic record must be accompanied by a Section 65B certificate to be admitted as evidence. The absence of this certificate would render the evidence inadmissible unless the party producing the evidence can prove its authenticity by other means.

The Court underscored three critical elements for electronic evidence admissibility:

1. Chain of Custody: The electronic record must be traced through a reliable chain of custody, proving that the data has not been altered from the time of its original creation to its presentation in court.
2. Integrity of the Data: The evidence must maintain its original state, ensuring it is free from tampering, deletion, or modification.
3. Certification under Section 65B: A certificate signed by an authorized person must accompany the electronic evidence, specifying the nature of the device or system used, the manner of the data's collection, and the integrity of the record.

The judgment also emphasized that the certificate under Section 65B should comply with the exact language prescribed by the statute to avoid ambiguity. This precision ensures uniformity in handling digital evidence and prevents evidentiary disputes.

Implications of Anvar Judgment

The Anvar decision has created a strict, uniform standard for the admissibility of electronic evidence, strengthening the evidentiary framework and safeguarding against the misuse of digital records. However, it has also introduced practical challenges, especially for law enforcement agencies and litigants unfamiliar with technical requirements.

Failure to produce a valid Section 65B certificate can lead to exclusion of critical evidence, potentially impacting the outcome of cases involving electronic communications, CCTV footage, emails, mobile messages, digital contracts, and forensic data from electronic devices.

Challenges in Practical Application

Several challenges arise in the application of Section 65B:

Lack of Technical Expertise: Many courts and lower judiciary members lack specialized knowledge of digital forensics, leading to difficulties in assessing the authenticity of electronic evidence.

Procedural Delays: Obtaining the necessary certificates and maintaining chain of custody can be time consuming, impacting the efficiency of trials.

Uniformity Issues: Different states and investigative agencies follow varying protocols for data collection and certification, causing inconsistency in evidence handling.

Data Preservation: Digital data can be volatile and ephemeral. Ensuring timely preservation and preventing deletion or overwriting is a constant challenge.

Addressing these issues requires systematic reforms, standardized procedures, and capacity building within the judiciary and law enforcement.

Striking the Balance: Policy Recommendations and Best Practices

The use of digital surveillance and electronic evidence involves a delicate balance between protecting national security and safeguarding individual rights such as privacy, free speech, and due process. To create a fair, transparent, and effective surveillance and evidence framework, India must consider the following policy recommendations and best practices:

1. Clear Legislative Framework for Surveillance

India urgently needs comprehensive legislation that clearly delineates the scope, limits, and conditions under which surveillance can be conducted. This law should:

Define the types of surveillance permitted, such as interception, tracking, metadata collection, and data mining.

Establish strict criteria of necessity and proportionality to ensure surveillance is conducted only when absolutely required for legitimate state interests like national security or serious crimes.

Mandate prior judicial authorization or approval by a designated independent authority before any surveillance operation commences.

Prohibit mass or indiscriminate surveillance practices that target the general population without suspicion.

Such a framework would provide legal clarity, prevent arbitrary or unauthorized surveillance, and align with constitutional protections.

2. Independent Oversight Mechanism

Surveillance activities must be subject to rigorous oversight by an independent body, separate from the executive and law enforcement. This body should:

Review and approve surveillance requests, ensuring adherence to legal standards.

Monitor the implementation of surveillance operations, preventing abuse or scope creep.

Receive complaints and conduct investigations into alleged violations.

Publish regular transparency reports on surveillance activities, maintaining public

accountability while safeguarding sensitive information.

Independent oversight would help build public trust and ensure that surveillance powers are not misused.

3. Uniform Evidence Handling Protocols

The collection, preservation, and presentation of electronic evidence must follow uniform, standardized protocols nationwide. This includes:

Establishing comprehensive guidelines on maintaining the chain of custody, forensic examination, and certification of electronic evidence.

Ensuring digital data is preserved immediately upon seizure or detection to prevent loss or alteration.

Using internationally accepted forensic tools and methods for evidence extraction and analysis.

Training law enforcement personnel and forensic experts in digital evidence handling and cybersecurity.

Uniformity would reduce procedural lapses, enhance evidence reliability, and facilitate smoother judicial proceedings.

4. Judicial Capacity Building

Judges and magistrates need ongoing training to understand the technicalities of digital evidence and surveillance laws. This would enable them to:

Scrutinize the authenticity and admissibility of electronic evidence effectively.

Ensure that surveillance authorizations comply with constitutional standards.

Balance national security interests with privacy and free speech rights when adjudicating surveillance related cases.

Empowered judiciary will serve as a strong check on potential governmental overreach.

5. Transparency and Public Participation

Transparency is vital to preventing abuse and maintaining democratic accountability. India should:

Mandate periodic publication of surveillance statistics, including the number of interception orders, authorizations granted, and types of crimes targeted.

Involve civil society organizations and privacy advocates in consultations on surveillance policy and legal reforms.

Educate the public about their rights and the limits of state surveillance, fostering awareness

and vigilance.

Public scrutiny and participation can act as powerful deterrents against unauthorized surveillance.

6. Adoption of Data Protection Principles

Although India's Personal Data Protection Bill is still evolving, integrating its principles into surveillance and evidence laws is essential. This includes:

Data minimization: Collect only the data strictly necessary for the surveillance purpose.

Purpose limitation: Use data collected solely for the authorized purpose.

Accountability: Ensure agencies handling data are accountable for breaches or misuse.

Rights of individuals: Provide mechanisms for individuals to access, correct, or challenge data held about them.

Applying these principles would align surveillance practices with global privacy standards.

7. Learning from Global Best Practices

India can draw from global frameworks such as the European Union's General Data Protection Regulation (GDPR) and the United Kingdom's Investigatory Powers Act (IPA), which include:

Robust judicial and parliamentary oversight.

Clear procedural safeguards for interception and data retention.

Independent commissioners overseeing surveillance activities.

Mandatory transparency reports and public disclosures.

Adapting these best practices in the Indian context would strengthen constitutional protections while enabling effective law enforcement.

Conclusion

The interplay between digital surveillance, privacy, and national security presents a complex and dynamic challenge for India's constitutional democracy. While the state must be empowered to protect its citizens from threats, it must do so without compromising fundamental rights guaranteed by the Constitution. The Indian judiciary's recognition of privacy as a fundamental right and its insistence on necessity, proportionality, and judicial oversight in surveillance activities set a clear constitutional mandate.

However, constitutional principles alone are insufficient without comprehensive legislative

reform, capacity building, and transparent governance mechanisms. The legal framework governing electronic evidence must be strengthened and uniformly implemented to ensure that digital records admitted in court meet the highest standards of authenticity and reliability. Surveillance laws must be clear, restrictive, and subject to independent oversight to prevent abuse and preserve democratic freedoms.

A well balanced digital surveillance regime is achievable through continuous legal clarity, judicial vigilance, training and technical expertise, transparency, and civic engagement. Only by embedding accountability, proportionality, and respect for privacy deeply within its laws and practices can India navigate the complexities of the digital age, safeguarding both its national security and the constitutional rights of its people.