RIGHT TO PRIVACY VS. STATE SURVEILLANCE - ANALYZING PROCEDURAL SAFEGUARDS AND STATE ACCOUNTABILITY IN THE AGE OF ADVANCED DIGITAL SURVEILLANCE

Roshani Pal[1] & Lalit Shukla[2]

ABSTRACT

The exponential growth of digital technologies has transformed governance, security, and public administration in unprecedented ways. Simultaneously, it has significantly expanded the surveillance capabilities of the modern state, thereby raising profound constitutional concerns relating to the right to privacy, civil liberties, human dignity, and democratic accountability. This paper critically examines the complex tension between the fundamental right to privacy and the increasing reliance on state surveillance mechanisms, with particular emphasis on procedural safeguards and institutional accountability in the deployment of advanced digital surveillance tools. These tools include mass data interception frameworks, large-scale biometric databases, facial recognition technologies, algorithmic profiling, and artificial intelligence-driven predictive analytics used for law enforcement and governance purposes.

Anchored in constitutional jurisprudence and evolving judicial interpretations of privacy as a fundamental right, the paper traces the doctrinal development of privacy protection in India. It situates the Indian experience within a comparative constitutional framework by analysing regulatory approaches adopted in the United States and the European Union, especially concerning data protection, proportionality standards, and independent oversight structures. The research further evaluates the adequacy of existing statutory regimes such as the Indian Telegraph Act, 1885, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, while also engaging with international human rights standards relating to surveillance, necessity, and due process.

The study argues that although national security, crime prevention, and maintenance of public order constitute legitimate state objectives,

[1] Post-Graduate in Law (LL.M.), Atal Bihari Vajpayee School of Legal Studies, Chhatrapati Shahu Ji Maharaj University, Kanpur
[2] Graduate in Law (LL.B.), Chhatrapati Shahu Ji Maharaj University, Kanpur

surveillance practices must be circumscribed by robust procedural guarantees rooted in legality, necessity, proportionality, transparency, and accountability. It highlights the risks of function creep, mass profiling, and algorithmic bias in the absence of effective regulatory frameworks. The paper concludes by proposing normative and institutional reforms including strengthened judicial authorization mechanisms, enhanced parliamentary scrutiny, mandatory technological impact assessments, periodic independent audits, and accessible remedies for rights violations. Ultimately, the research seeks to contribute to the ongoing discourse on reconciling technological governance with constitutional freedoms, emphasizing that privacy has become an indispensable component of individual autonomy and democratic legitimacy in the contemporary digital age.

Keywords: Right to Privacy, State Surveillance, Proportionality, Digital Surveillance, Constitutional Law, Data Protection, Procedural Safeguards, Accountability, National Security.

INTRODUCTION

The 21st century has witnessed the transformation of surveillance from a targeted law enforcement technique into a sophisticated digital ecosystem capable of monitoring populations on a scale. Governments today deploy advanced technologies including metadata collection, biometric identification systems, internet traffic monitoring, automated facial recognition, and AI-enabled predictive policing tools. While these tools promise enhanced national security and efficient governance, they simultaneously pose unprecedented threats to individual autonomy, informational self-determination, and democratic freedoms.

In constitutional democracies, the right to privacy functions as a structural limitation on state power. In India, this right was authoritatively recognized as a fundamental right under Art. 21 of the Constitution in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[3] The judgment marked a doctrinal shift, elevating privacy to the status of a constitutional guarantee intertwined with dignity, liberty, and autonomy.

However, recognition of privacy as a fundamental right does not eliminate the state's authority to conduct surveillance. Rather, it demands that surveillance regimes operate within constitutionally permissible boundaries. The central question is not whether the state may surveil, but under what conditions and with what safeguards. This paper explores the normative

[3] (2017) 10 SCC 1.

and procedural architecture required to reconcile privacy with legitimate state interests.[4]

CONCEPTUAL FOUNDATIONS - PRIVACY AND SURVEILLANCE

The Constitutional Meaning of Privacy

Privacy has evolved from a narrow protection against physical intrusion into a multidimensional right encompassing bodily integrity, informational control, decisional autonomy, and spatial privacy. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[5] court recognized privacy as intrinsic to life and personal liberty under Art. 21, as well as to freedoms under Part III of the Constitution. The Court articulated three broad aspects of privacy -

- **Bodily Privacy** – protection from physical intrusion.
- **Informational Privacy** – control over dissemination and processing of personal data.
- **Decisional Autonomy** – freedom to make intimate personal choices.

The informational dimension is particularly significant in the digital era, where surveillance is no longer limited to physical monitoring but extends to metadata, online communications, geolocation tracking, and algorithmic profiling.

The Court further established a structured proportionality test requiring that any invasion of privacy must satisfy legality (existence of law), legitimate state aim, rational nexus, necessity and proportionality, and procedural safeguards against abuse. This test has become the constitutional yardstick for evaluating surveillance frameworks.

The Nature of Modern Digital Surveillance

Unlike traditional wiretapping, contemporary surveillance operates through bulk metadata collection, deep packet inspection, biometric identification systems, facial recognition in public spaces, and AI-driven predictive analytics. Surveillance has shifted from reactive investigation to preventive and predictive governance. This transformation challenges conventional legal doctrines premised on individualized suspicion and targeted warrants.

The concern lies not merely in data collection but in aggregation and profiling. As observed in

[4] David Gray & Danielle Keats Citron, *"The Right to Quantitative Privacy"*, 98 Minn. L. Rev. 62 (2013).
[5] (2017) 10 SCC 1.

Kharak Singh v. State of Uttar Pradesh,[6] even surveillance without physical intrusion can violate personal liberty. Later jurisprudence expanded this understanding to informational domains.

An important dimension of contemporary surveillance that warrants consideration is the growing role of private corporations in the collection, processing, and commercialization of personal data. Modern digital ecosystems are structured around extensive data extraction practices, often described as "surveillance capitalism," where personal information is treated as an economic resource. Technology companies routinely collect vast quantities of behavioral data through online platforms, mobile applications, and digital services, generating detailed profiles of individuals' preferences, habits, and social interactions.

This corporate accumulation of personal data has significant implications for state surveillance. Governments increasingly rely on private intermediaries such as telecommunications providers, internet platforms, and data analytics firms for access to user information. The resulting public–private surveillance nexus blurs traditional distinctions between state action and private data processing. While constitutional safeguards typically regulate state conduct, indirect access to privately collected data may enable governments to circumvent stricter constitutional limitations.

The informational asymmetry created by such practices raises concerns regarding meaningful consent and informational self-determination. Individuals frequently lack knowledge of the extent to which their personal data is collected, stored, and shared. Standardized privacy policies and opaque data-processing mechanisms undermine the autonomy that privacy seeks to protect. Consequently, the conceptual understanding of privacy must expand beyond protection against direct state intrusion to include safeguards against excessive data extraction by private entities that facilitate state surveillance.[7]

Furthermore, large-scale data aggregation enables predictive governance techniques that rely on algorithmic inference rather than direct observation. These practices generate probabilistic assessments of behavior, risk, and identity, which may be used for law enforcement or administrative decision-making. Such developments challenge traditional legal frameworks premised on individualized suspicion and reinforce the need for robust regulatory oversight

[6] AIR 1963 SC 1295.
[7] *Supra* note 2.

governing both public and private actors engaged in surveillance-related activities.

LEGAL FRAMEWORK GOVERNING SURVEILLANCE IN INDIA

Statutory Framework

Section 5(2) of Indian Telegraph Act, 1885 permits interception of communications on grounds such as public emergencies or public safety. However, the language is broad and predates digital communications. In *People's Union for Civil Liberties (PUCL) v. Union of India*,[8] court laid down procedural safeguards for telephone tapping, including Home Secretary authorization, Limited duration, Periodic review committee oversight, and Record maintenance. While significant, these guidelines were formulated in an era of landline interception, not mass digital surveillance.

Section 69 of IT Act, 2000 authorizes interception, monitoring, and decryption of digital information for specified grounds including sovereignty and public order. The IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 provide procedural requirements similar to those under PUCL, but concerns remain regarding executive-dominated authorization, lack of judicial pre-approval, and limited transparency.

The DPDPA, 2023 introduces data processing principles but contains broad exemptions for the State in the interest of sovereignty and public order. Such exemptions raise questions regarding proportionality and accountability.

Constitutional Judicial Review of Surveillance

In *Anuradha Bhasin v. Union of India*,[9] court held that internet shutdowns must satisfy proportionality and be subject to periodic review. Although not directly a surveillance case, it reinforced the necessity of procedural safeguards in digital governance. Similarly, in *Maneka Gandhi v. Union of India*,[10] court expanded Art. 21 by requiring that any deprivation of liberty must be "just, fair and reasonable." This principle now informs the constitutional validity of surveillance laws. The proportionality doctrine was further elaborated in *Modern Dental College v. State of Madhya Pradesh*,[11] where court adopted a structured proportionality

[8] (1997) 1 SCC 301.
[9] (2020) 3 SCC 637.
[10] (1978) 1 SCC 248.
[11] (2016) 7 SCC 353.

analysis, later reaffirmed in Puttaswamy's ruling.

COMPARATIVE CONSTITUTIONAL APPROACHES TO SURVEILLANCE AND PRIVACY

The constitutional balancing of privacy and surveillance has evolved differently across jurisdictions, yet certain core principles such as legality, necessity, proportionality, and independent oversight recur across democratic systems. A comparative analysis of the US & EU provides valuable insight into how constitutional democracies structure safeguards against excessive state intrusion in the digital era.

In US, privacy protection against surveillance is primarily grounded in the Fourth Amendment to the Constitution, which guards against unreasonable searches and seizures. The jurisprudence historically revolved around physical trespass, but it evolved in response to technological changes. In *Katz v. United States*,[12] court shifted the doctrinal basis from property to a "reasonable expectation of privacy" test, holding that wiretapping a public phone booth constituted a search within the meaning of the Fourth Amendment. This marked a foundational recognition that privacy extends beyond physical intrusion.

However, the third-party doctrine, articulated in *Smith v. Maryland*,[13] limited privacy claims over metadata voluntarily shared with service providers. In the digital age, this doctrine proved controversial because individuals routinely share vast amounts of data with intermediaries. Recognizing the implications of technological aggregation, court in *Carpenter v. United States*,[14] held that acquisition of historical cell-site location information constitutes a search requiring a warrant. Carpenter signaled judicial sensitivity to the pervasive tracking potential of digital technologies and indicated a partial retreat from the rigid application of the third-party doctrine.

In contrast, EU has adopted a more structurally robust privacy regime rooted in human dignity and data protection as fundamental rights. Art. 7 & 8 of the Charter of Fundamental Rights of EU explicitly guarantee respect for private life and protection of personal data. The jurisprudence of Court of Justice of the EU has consistently imposed strict proportionality

[12] 389 U.S. 347 (1967).
[13] 442 U.S. 735 (1979).
[14] 585 U.S. ___ (2018).

standards on state surveillance. In *Digital Rights Ireland Ltd v. Minister for Communications*,[15] court invalidated the Data Retention Directive on the ground that indiscriminate retention of telecommunications data violated fundamental rights. Similarly, in *Tele2 Sverige AB v. Post-och telestyrelsen*,[16] court ruled that general and indiscriminate data retention regimes were incompatible with EU's law. The EU model emphasizes independent supervisory authorities, judicial authorization, and strict necessity tests.

India's constitutional framework, particularly after *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[17] aligns more closely with the European proportionality model than with the traditional American approach. Puttaswamy's ruling expressly adopted a structured proportionality test, thereby constitutionalizing the requirement that surveillance measures must be narrowly tailored and accompanied by procedural safeguards. However, unlike the EU system, India's statutory surveillance architecture remains predominantly executive-controlled, raising concerns about effective oversight.

Beyond domestic constitutional frameworks, international human rights law provides normative guidance on the permissible limits of surveillance. The right to privacy is recognized under Article 12 of UDHR and Article 17 of ICCPR, which prohibit arbitrary or unlawful interference with privacy, family, home, or correspondence. These provisions impose both negative and positive obligations on states to prevent unjustified intrusions and establish effective legal protection.

International human rights bodies have emphasized that surveillance measures must conform to principles of legality, necessity, and proportionality. The legality requirement mandates that surveillance practices be grounded in accessible and foreseeable laws that clearly define the scope of state authority. Secret or vague legal frameworks fail to meet this standard because they undermine predictability and democratic accountability.

The necessity requirement further restricts surveillance to measures that address pressing social needs, such as national security or prevention of serious crime. States must demonstrate that less intrusive alternatives are insufficient to achieve the intended objective. Proportionality requires a careful balancing of individual rights against collective interests, ensuring that the

[15] Joined Cases C-293/12 and C-594/12 (2014).
[16] Joined Cases C-203/15 and C-698/15 (2016).
[17] (2017) 10 SCC 1.

extent of intrusion is not excessive relative to the objective pursued.

The UNHRC has repeatedly expressed concern regarding mass surveillance programs that involve indiscriminate data collection or bulk interception of communications. Such practices are considered incompatible with the requirement of targeted and proportionate interference. International jurisprudence thus reinforces the principle that surveillance must be exceptional rather than routine.

For India, international human rights norms serve as interpretive tools in constitutional adjudication. The integration of global standards within domestic constitutional reasoning strengthens the legitimacy of privacy protection and aligns national surveillance practices with universally recognized principles of human dignity and personal autonomy.

THE DOCTRINE OF PROPORTIONALITY AND PROCEDURAL SAFEGUARDS

The doctrine of proportionality has emerged as the central constitutional mechanism for reconciling privacy with surveillance. In *Modern Deexists ande v. State of Madhya Pradesh*,[18] court formally adopted the four-pronged proportionality test, requiring that state action must pursue a legitimate aim, be suitable to achieve that aim, be necessary in that no less restrictive alternative exists and maintains a balance between the extent of rights infringement & public interest served. This framework was affirmed and elevated in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[19]

The legality requirement mandates that surveillance must be backed by clear, accessible, and precise legislation. Vague or overly broad statutory provisions fail to meet constitutional scrutiny. Court's decision in *Shreya Singhal v. Union of India*,[20] although dealing with freedom of speech under Sec. 66A of the IT Act, 2000 is instructive for surveillance jurisprudence. Court struck down the provision due to vagueness and chilling effects, emphasizing that laws affecting fundamental rights must provide clear standards. Surveillance statutes that confer wide discretionary power without narrowly defined thresholds risk similar constitutional infirmity.

The necessity requirement compels the state to demonstrate that surveillance is indispensable

[18] (2016) 7 SCC 353.
[19] (2017) 10 SCC 1.
[20] (2015) 5 SCC 1.

for achieving a legitimate objective such as national security or prevention of serious crime. Blanket or indiscriminate data collection mechanisms rarely satisfy this threshold. In *Anuradha Bhasin v. Union of India*,[21] court held that restrictions affecting digital rights must be proportionate and periodically reviewed. Although concerning internet shutdowns, the reasoning underscores that digital governance measures must not exceed what is strictly required.

Proportionality in a strict sense requires balancing the gravity of intrusion against the importance of the state objective. Mass surveillance regimes, by their very architecture, often lack individualized suspicion and thereby heighten the risk of disproportionate interference. The informational privacy concerns articulated in Puttaswamy's ruling stress that aggregation of personal data can reveal intimate patterns of life, thereby intensifying the constitutional stakes.

Procedural safeguards are the operational dimension of proportionality. In *People's Union for Civil Liberties (PUCL) v. Union of India*,[22] court recognized that the absence of procedural checks renders surveillance susceptible to abuse. Court mandated prior authorization by a senior executive authority and review by a committee. While this framework represented progress at the time, contemporary digital surveillance technologies have expanded in scale and complexity, necessitating more robust mechanisms such as prior judicial authorization, independent regulatory oversight, transparency reports, and ex-post remedies.

Judicial pre-authorization serves as a critical safeguard because it introduces independent scrutiny before intrusion occurs. Comparative systems, particularly in Europe, treat judicial authorization as an essential feature of lawful interception. In India, interception approvals remain executive-centric, raising concerns about concentration of power. The principle articulated in *Maneka Gandhi v. Union of India*,[23] that procedure must be fair, just, and reasonable, which implies that independent oversight is integral to constitutional compliance.

EMERGING TECHNOLOGIES & CHALLENGES TO ACCOUNTABILITY

Advanced digital surveillance technologies complicate traditional accountability frameworks. Artificial intelligence systems deployed for predictive policing, facial recognition in public

[21] (2020) 3 SCC 637.
[22] (1997) 1 SCC 301.
[23] (1978) 1 SCC 248.

spaces, and automated risk assessment tools operate through algorithmic decision-making processes that are often opaque. The opacity of algorithms undermines transparency and impedes meaningful judicial review.

Facial recognition technology exemplifies this challenge. When deployed in public spaces without clear legislative backing or oversight, it risks transforming public anonymity into permanent traceability. The chilling effect on free movement and expression cannot be understated. Court's reasoning in *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*,[24] which upheld the Aadhaar scheme with limitations, illustrates court's willingness to examine technological architectures closely. The majority emphasized purpose limitation, data minimization, and oversight mechanisms, while striking down provisions that enabled private sector access and indefinite data retention. The ruling demonstrates that technological infrastructure must incorporate constitutional safeguards at the design stage.

Mass data aggregation also heightens risks of profiling and discrimination. Surveillance data, when combined with AI analytics, can produce predictive models that disproportionately target marginalized communities. Constitutional commitments to equality under Art. 14 intersect with privacy concerns, creating a layered constitutional analysis. The absence of algorithmic transparency undermines the ability of individuals to challenge adverse outcomes, thereby weakening accountability.

State accountability further requires effective remedies. The right to constitutional remedies under Art. 32, recognized as the "heart and soul" of Indian Constitution in *L. Chandra Kumar v. Union of India*,[25] ensures judicial review of state action. However, covert surveillance often remains undisclosed, preventing individuals from knowing that their rights have been infringed. Without notification mechanisms or transparency obligations, remedies remain largely theoretical.

The DPDPA, 2023 introduces data protection principles but provides broad exemptions to state agencies. Exemptions without narrowly tailored safeguards risk diluting the proportionality framework articulated in Puttaswamy's ruling. Effective accountability demands independent data protection authorities, parliamentary scrutiny, audit requirements, and transparency

[24] (2019) 1 SCC 1.
[25] (1997) 3 SCC 261.

reporting obligations.[26]

The increasing reliance on algorithmic systems in surveillance and governance raises significant due process concerns. Automated decision-making tools are often deployed in predictive policing, risk assessment, and identity verification processes. While such technologies promise efficiency and objectivity, they may also embed biases within their design and operation. Algorithms trained on historical data may reproduce patterns of discrimination, disproportionately affecting vulnerable or marginalized populations.

A central challenge lies in the opacity of algorithmic systems. Many artificial intelligence models operate as "black boxes," making it difficult to understand how decisions are generated. This lack of transparency undermines procedural fairness by preventing individuals from challenging adverse outcomes or verifying the accuracy of data used in decision-making processes. The absence of explainability further complicates judicial review, as courts may lack the technical expertise required to assess algorithmic functioning.

Due process in a constitutional democracy requires notice, opportunity to be heard, and reasoned decision-making. When surveillance-based decisions are automated without adequate human oversight, these procedural guarantees may be compromised. The risk is particularly pronounced where algorithmic outputs directly influence law enforcement actions, access to public services, or regulatory interventions.

To address these concerns, regulatory frameworks must incorporate principles of algorithmic accountability, including transparency obligations, audit mechanisms, and human oversight requirements. Impact assessments evaluating the potential consequences of surveillance technologies can further enhance accountability. Embedding constitutional values within technological design, often described as "privacy by design", ensures that surveillance infrastructures respect fundamental rights at the operational level.

STATE ACCOUNTABILITY AND DEMOCRATIC OVERSIGHT IN SURVEILLANCE REGIMES

State accountability constitutes the normative core of any constitutional democracy, particularly where coercive or intrusive powers are exercised in secrecy. Surveillance, by its very nature, operates covertly and asymmetrically, placing the individual in a structurally

[26] Daniel J. Solove, *"A Taxonomy of Privacy"*, 154 U. Pa. L. Rev. 477 (2006).

vulnerable position vis-à-vis the state. In such a context, procedural safeguards are not merely technical requirements but constitutional imperatives that ensure fidelity to the rule of law.

The recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[27] fundamentally altered the constitutional landscape by embedding informational self-determination within Art. 21. Court emphasized that privacy is essential to dignity, liberty, and autonomy, and that state action infringing upon it must withstand strict scrutiny under the proportionality doctrine. Implicit in this framework is the necessity of institutional mechanisms that prevent arbitrary surveillance and provide meaningful recourse in cases of abuse.

One of the central weaknesses in contemporary surveillance regimes lies in executive concentration of authorization powers. Under the Telegraph Act & IT Act, 2000, interception orders are typically issued by executive authorities, subject to internal review mechanisms. While *People's Union for Civil Liberties (PUCL) v. Union of India*,[28] introduced procedural safeguards, including review committees, these remain largely executive-driven. The absence of mandatory prior judicial authorization raises concerns regarding impartial oversight. Constitutional jurisprudence, particularly the expanded interpretation of "procedure established by law" in *Maneka Gandhi v. Union of India*,[29] requires that procedures affecting personal liberty must be fair, just, and reasonable. A system in which the executive authorizes and reviews its own surveillance decisions risks failing to this standard.

Judicial oversight serves as an institutional counterbalance. In democracies where surveillance warrants require prior judicial approval, an independent authority evaluates necessity and proportionality before intrusion occurs. Such pre-authorization mechanisms ensure that surveillance is targeted rather than indiscriminate. The reasoning adopted in *Anuradha Bhasin v. Union of India*,[30] which mandated publication and review of internet shutdown orders, reflects judicial insistence on transparency and reviewability.

Parliamentary oversight constitutes another dimension of democratic accountability. Surveillance frameworks often involve classified operations, but this does not negate the need for legislative supervision. Parliamentary committees with security clearances can examine compliance, audit practices, and evaluate the proportionality of surveillance programs. Without

[27] (2017) 10 SCC 1.
[28] (1997) 1 SCC 301.
[29] (1978) 1 SCC 248.
[30] (2020) 3 SCC 637.

such scrutiny, surveillance risks expanding beyond its originally sanctioned objectives, a phenomenon commonly described as "function creep".

Transparency, though inherently limited in matters of national security, remains a critical safeguard. Aggregate transparency reports, declassified policy guidelines, and statistical disclosures regarding interception orders can promote public trust without compromising operational details. Court's reasoning in *Shreya Singhal v. Union of India*,[31] recognized the chilling effect that vague and overbroad legal provisions can have on constitutional freedoms. Secretive surveillance regimes may similarly chill free speech and association if individuals fear constant monitoring.

An additional element of accountability concerns remedies. The constitutional architecture under Art. 32 & 226 ensures judicial review of rights violations. In *L. Chandra Kumar v. Union of India*,[32] court reaffirmed the centrality of judicial review as part of the basic structure of the Constitution. However, covert surveillance complicates access to remedies because affected individuals may never learn of the intrusion. International best practices increasingly recommend post-surveillance notification once operational risks subside.

The DPDPA, 2023 establishes a Data Protection Board, but the breadth of exemptions granted to state agencies raises questions regarding its effectiveness in overseeing surveillance activities. The proportionality test articulated in *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*,[33] emphasized data minimization, purpose limitation, and storage restrictions.

CONCLUSION & A WAY FORWARD

The rapid evolution of digital surveillance technologies has fundamentally altered the relationship between the individual & state. Surveillance is no longer limited to targeted interception but encompasses vast networks of data collection, biometric identification, and algorithmic profiling. In this transformed landscape, the right to privacy operates as a constitutional bulwark against unchecked state power. Comparative constitutional experiences from the US & EU reveal that robust oversight mechanisms, independent supervisory authorities, and strict necessity tests are essential to maintaining democratic legitimacy. The Indian constitutional framework, particularly after Puttaswamy, possesses the doctrinal tools

[31] (2015) 5 SCC 1.
[32] (1997) 3 SCC 261.
[33] (2019) 1 SCC 1.

required to regulate surveillance effectively.

Strengthening judicial authorization procedures, enhancing parliamentary oversight, mandating transparency reporting, establishing independent auditing of surveillance technologies, and ensuring effective remedies are indispensable steps toward reconciling security imperatives with constitutional freedoms. Surveillance cannot be eliminated in a complex security environment, but it can and must be disciplined by law. In the age of advanced digital surveillance, the true test of constitutionalism lies not in the absence of state power but in its restraint. A democracy committed to dignity and liberty must ensure that surveillance remains exceptional, accountable, and proportionate.