The Right to Fair Trial in The Digital Age: A Critical Analysis of Criminal Procedure in the Era of Technological Surveillance

Gargesh Kumar* & Prof. (Dr.) Anand Kumar Vishwakarma**

ABSTRACT

The introduction of digital technologies into criminal justice systems has greatly changed the way of investigations, gathering evidence, and methods of prosecution. Although technologies like CCTV surveillance, electronic interception, facial recognition, and data analytics have enhanced the effectiveness of the investigation, they have posed complex issues to procedural fairness and the safeguarding of fair trial rights. The major issue discussed in this paper is to answer the following question: how do contemporary surveillance technologies influence the right to a fair trial of a person in India? It only selectively addresses the initial phases of investigation, before the trial has commenced, and examines the applicability of these high-tech practices within the evolving Indian legal system. It follows a socio-legal and constitutional paradigm of studying major legislations such as the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, Bharatiya Sakshya Adhiniyam (BSA), 2023 and the Digital Personal Data Protection Act (DPDP), 2023.

The paper will hold that despite the fact that digital surveillance has allowed better detection of crimes and the emergence of new mechanisms of participation and protection of the victims, these needs must be well balanced with the constitutional rights of the accused so as to have a holistic framework of Nyaya (justice). This trend towards automated and data-driven investigative procedures is worrying because of the prerequisites of transparency, accountability, and the loss of fundamental values such as the presumption of innocence, equality of arms, and the right to defence.

The paper also identifies the weaknesses of the current judicial investigation tools, especially when it comes to the application of dark technologies and minimal disclosures. It finds loopholes within the regulatory protections and emphasises a greater requirement of procedural controls, through the prism of doctrinal analysis and

* **Gargesh Kumar** is a Research Scholar at University of Lucknow, Lucknow
** **Prof. (Dr.) Anand Kumar Vishwakarma** is a Professor of Law, University of Lucknow, Lucknow

assessment of judicial responses. It concludes that technological improvement in criminal investigation is unavoidable, but it should be under strong law-based rights protection. To maintain the validity of the criminal justice system in the digital age, it is necessary to strengthen judicial scrutiny and increase transparency and accountability.

Keywords: *Fair Trial, Digital Surveillance, Criminal Procedure, Digital Evidence, Technological Policing.*

***

1. INTRODUCTION

The criminal justice system in the various jurisdictions is going through a radical change due to the accelerated technological change. The digital technologies have transformed the detection, investigation and prosecution of crimes, and their overall models of criminal proceedings have been completely transformed. Technological devices that used to be marginal to investigations, like electronic communication records, computer databases, and computerised surveillance systems, no longer hold a peripheral position in law enforcement. This has digitalised the investigative process, which has increased the investigative capacity; it has reshaped the dynamic between the State and the individual, specifically in the pre-trial process of criminal proceedings.[1]

The emergence of technological surveillance can be considered as one of the greatest modes of this change. Modern criminal investigations are becoming more heavily dependent on closed-circuit television (CCTV), telephone tapping, metadata-based location tracking, facial recognition and artificial intelligence-based analysis tools. The technologies allow gathering data on a large scale and continuously, and may not be limited to particular suspects or crimes. Although this type of surveillance is arguably necessary due to the complex and technologically facilitated nature of crime, it has become extremely widespread and therefore should be questioned in terms of transparency, accountability, and procedural fairness.[2] The change in the principle of targeted surveillance to large-scale, data-driven surveillance is a break in the traditional investigative traditions based on individualised suspicion.

[1] Andrew Ashworth and Lucia Zedner, 'Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure and Sanctions' (2008) 2 CLP 21

[2] Sandi YudhaPrayoga, 'The Criminal Justice System and Technology in the Digital Age' (2024) *Edunity* 551–552

It is on this basis that the right to a fair trial takes on new significance. The right to fair trial, which has a long history of being a pillar of criminal jurisprudence, guarantees that the person is not arbitrarily taken by the state and that a criminal justice system is working towards delivering justice and equality and in a way that does not violate the principle of due process. The courts have always believed that fairness is not limited to the courtroom but extends to investigative and pre-trial procedures, which determine the result of the trials.[3] Since the use of surveillance technologies is more and more affecting the amount of evidence and prosecutorial tactics, their alignment with the fair trial guarantees raises concrete attention.

This paper aims to critically analyse how technological surveillance affects criminal procedure under the right to a fair trial. It has as its main objective the analysis of the impact of surveillance-based investigation on such core principles as the presumption of innocence, equality of arms and procedural fairness. The research is confined to the doctrinal and analytical study of surveillance in the criminal justice systems, based on the court rulings and scientific literature. The paper will make a contribution to the dynamic discussion of the rights-based constraints of digital justice by examining the point of convergence between technology and fair trial rights.[4]

2. THEORETICAL FRAMEWORK: THE RIGHT TO FAIR TRIAL

2.1. Meaning and Evaluation of Fair Trial

The right to fair trial is among the underlying principles of criminal justice, which is based on the wider principles of natural justice, the rule of law, and the guard against arbitrary use of state power. The concept of fair trial evolved due to the coercive and biased adjudicatory practice, which is slowly gaining constitutional footing in constitutional provisions and international human rights documents. International law Foundational documents like the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights set forth that all humans should be able to have a fair and public hearing in front of a competent, independent, and impartial tribunal. These guarantees have since been stretched by judicial interpretation to include the pre-trial and investigative stages as well as the trial itself,

[3] *Maneka Gandhi v Union of India* AIR 1978 SC 597
[4] Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) 49 *Computer Law & Security Review* 105801

on the principle that procedural unfairness during the first stage of the criminal justice process is irreversible.[5]

The right to a fair trial has been construed out of the constitutional right of life and personal liberty in India, and courts have repeatedly stressed that fairness is not an a priori notion but one that has to respond to social and technological changes.[6] Such digitisation of criminal justice has consequently created the need to review the conventional conception of fairness in criminal procedure.

2.2. Essential Elements of the Right to Fair Trial.

2.2.1. Presumption of Innocence

The innocent housing presumption is the normative point of criminal determination and imposes the whole cost of proving guilt on the prosecution. This rule stipulates that one should be treated as innocent until he or she is proven guilty under a lawful procedure. It has always been emphasised by judicial interpretation that this presumption is not used only in adjudication but also in the investigation and collection of evidence.[7] Within the framework of data-driven investigations and digital surveillance, there is a growing threat of how algorithmic profiling and predictive technologies can undermine this assumption by prejudice-based enforcement as opposed to prosecution based on evidence.[8]

2.2.2. The Constitutional Right to be Heard

A key change in this evolving framework is seen in the participatory rights brought about under the Bharatiya Nagarik Suraksha Sanhita, 2023.[9] Section 360 BNSS, in particular, is that it requires the victim to have an opportunity to be heard before the State withdraws a prosecution. Such a provision is a historical leap forward, as the victim ceases to be an observer of the justice process but an active participant.[10]

---

[5] Universal Declaration of Human Rights 1948 art 10; International Covenant on Civil and Political Rights 1966 art 14

[6] Akhil Yadav and Devesh Shukla, 'A Critical Analysis on Right to Fair Trial under Indian Laws' (2024) International Journal of Creative Research Thoughts (IJCRT) 648–650

[7] *Id*

[8] Stoykova, (n 4) 2212–2215 .

[9] *Woolmington v Director of Public Prosecutions* [1935] AC 462 (HL)

[10] Andrew D Selbst and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87 FLR 1085

Other than Section 360, several additional clauses of the BNSS support this victim-focused and constitutionally appropriate strategy:

- **Section 183 BNSS (Medical examination of victim)**: Guarantees the sensitivity and dignity of procedures, especially in cases involving serious offences.[11]
- **Section 308 BNSS (Examination of accused):** Provisions of the accused: Guarantees to the accused the right to a fair hearing of the circumstances that emerge in the evidence against them.[12]
- **Section 230 BNSS (Supply of police report and documents)**: Assures transparency and enhances the right to fair defence.[13]

Together, these provisions reflect a mindful legislative attempt to reconcile two constitutional imperatives of protecting the presumption of innocence and meaningful victim participation. Section 360 in particular stands as a defining reform - the entrenchment of the constitutional right to be heard in procedural law and an indication of a move towards a more balanced and restorative system of justice.

In this way, the BNSS goes beyond a purely adversarial model and falls into a more comprehensive interpretation of Article 21 one that not only protects against wrongful conviction, but affirms the victim's right to dignity, participation and a fair investigative process, thus furthering a more holistic vision of Nyaya (justice).

2.2.3. Equality of Arms

The parity of arms is a vital provision of procedural fairness and requires that no party to a criminal action should be put at a considerable disadvantage. This principle stipulates that the defence should be given a reasonable chance to contest prosecution evidence and put its case across. The equality may be compromised in a technologically complicated case, especially when there is digital evidence or proprietary surveillance equipment, by the asymmetry of technical expertise and access to knowledge. According to scholars, these asymmetries are a

[11] Bharatiya Nagarik Suraksha Sanhita 2023, s 183
[12] *Id*
[13] *Id*

great danger to the protection of fair trial when courts and defence counsel do not have sufficient knowledge of the complex technologies used by the State.[14]

2.2.4. Right to Counsel or Legal Representation

The right to counsel is part and parcel of the fair trial rights. Availability of qualified legal services allows the accused to get familiar with the nature of the proceedings, put into question illegitimate investigative methods, and argue against the admissibility and dependability of evidence. The courts have appreciated that the absence of access to effective or timely legal assistance undermines the fairness of the process and undermines the validity of the criminal process.[15] These right gains an additional relevance in the digital-era prosecutions, where the representatives of law will have to be in a position to interact with the evidence that has been mediated by technology and surveillance-focused investigations.

2.2.5. Due Process and Procedural Fairness

Due process reflects the more general premise that criminal action be administered in line with the clearly reasonably set out legal procedures that are not arbitrary, unenlightened, or unfair. Procedural fairness requires the legality of authorising investigative action, evidentiary standards, and the presence of significant judicial control. The growing use of digital technologies in the investigation of crimes has revealed holes across the procedural protective measures, provoking the fear of uncontrolled executive discretion and the impossibility of challenging the evidence created by technology.[16]

2.2.6. Fair Trial: A Non-Derogative Human Right

The right to a fair trial is commonly understood as a non-derogable human right and one of the fundamental elements of the rule of law. The critical aspects of fairness, impartiality and due process cannot be completely suspended even in a case of a national security concern or a public emergency. Even in judicial and scholarly discussion, it is always affirmed that efficiency and technological progress or security interests cannot be used as a pretext to water down basic procedural safeguards.

[14] Bart Custers, 'A Fair Trial in Complex Technology Cases: Why Courts and Judges Need a Basic Understanding of Complex Technologies' (2024) 52 Computer Law & Security Review 105935, 1–3
[15] Yadav and Shukla, (n 6) 651–652
[16] Prayoga, (n 2) 550–552

2.2.7. Fair Trial and Criminal Procedure Relationship.

Criminal procedure is the main way in which the principles of fair trial are changed into enforceable rights. Abstract constitutional and human rights are operationalised by procedural regulations that control investigation, evidence and adjudication. This relationship has since become more complicated in the digital era, with the conventional procedural structures unable to adapt to the techno-logicalized method of surveillance and the digital evidence. The fact that criminal procedure must develop in the same direction as fair trial guarantees that it will therefore be fundamental in the protection of individual rights, in addition to the legitimacy of the criminal justice system.[17]

3. Criminal Justice And Technological Surveillance

3.1. Concept and Scope

Technological surveillance can be viewed as a combination of two types of surveillance, namely: Technological Surveillance and Surveillance of Technology. Technological Surveillance can be taken as a synthesis between two forms of surveillance, specifically: Technological Surveillance and Surveillance of Technology.

Technological surveillance in criminal justice refers to an organised application of computer systems and robotic devices by police to monitor, gather and examine data useful in the control and investigation of crime. In contrast to the traditional surveillance, where physical security and human intelligence became the main elements of surveillance, contemporary surveillance is carried out by means of technological infrastructures that are embedded and constantly generate and process information.[18] The growing invisibility and scale of this type of surveillance have, to a certain degree, broadened the scope of criminal investigations and, at the same time, diminished transparency as to how data are collected and used. Legal scholarship notes that this has erased the difference between targeted investigations and generalised monitoring and made state power wider in the criminal process.

[17] Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) Computer Law & Security Review 49, 2215–2218
[18] *Id*

Technological surveillance does not involve serious crime-related activities or extraordinary situations anymore; it is a part and parcel of daily policing and administration of criminal justice.

3.2. Electronic Surveillance and Interception.

In modern criminal justice systems, the use of electronic surveillance has become the focus of the investigation procedure. It includes the interception of telephonic communications, email, messaging on the internet, and the Internet. Due to the rapid development of communication technologies, law enforcement agencies can now easily track communications in real time and retrospectively, which has greatly increased the volume, availability and evidence quality of such information.[19]

This transformation is currently governed in India by the Telecommunications Act 2023,[20] read alongside the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024.[21] These frameworks are the statutory basis for lawful interception, and include procedural safeguards on how it is to be used to prevent misuse. The 2024 Rules in particular include requirements for prior authorisation by competent authorities, recording of reasons in writing, limitation of interception to certain grounds, such as national security and public order, and provision for periodic review by oversight committees.[22] The inclusion of such principles as necessity, proportionality, and limitation of data retention reflects an effort to limit the use of surveillance measures to the extent permitted by Article 21(2)4, namely in accordance with the principles of necessity and proportionality.[23]

Nevertheless, even with these precautions, there are fears. Scholars have pointed out that procedural protections are often hard-pressed to keep up with the substantial technological progress and thus are at risk of executive power runaway and a lack of transparency in authorisation processes.[24] The magnitude and invisibility of digital surveillance put the imbalance between state power and individual privacy rights in a further precarious position.

---

[19] Orin S Kerr, 'Internet Surveillance Law after the USA FREEDOM Act' (2015) 72 *Washington and Lee Law Review* 643
[20] Telecommunications Act 2023 (India)
[21] Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024 (India).
[22] ibid rr 3–7
[23] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[24] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001)

Meanwhile, the admissibility and ease of access to electronically intercepted information have radically redefined the practice of evidence. The normalised use of intercepted communications signals the beginning of a new era in investigative case law, where intercepted communications will be considered a normal part of the prosecution strategy rather than an exceptional investigative tool that is only used in exceptional instances to protect the right to a fair trial and civil liberties.

3.3. CCTV and Mass Surveillance

The spread of CCTV systems and visual surveillance systems has been one of the factors that gave rise to the mass surveillance of areas with crowds and semi-crowds. Such systems are more interconnected and have long-term data storage capabilities, which makes them trace the movements of individuals. The academic discussion provides that although CCTV is often defended as a tool of crime deterrence, its development with sophisticated analytics has added to its scope of activity from observation to recognition and tracking of behaviour.[25] This growth brings up the issues of proportionality and progressive normalisation of the always-on surveillance, especially where there are no explicit statutory boundaries to how long visual data can be kept, accessed and used secondarily.

3.4. Digital Forensics and Metadata.

Digital forensics has become an essential part of a criminal investigation in the age of the prevalence of digital devices. Police regularly use information gleaned from mobile handsets, computers and the internet to recreate time chains, chart associations and spot trends. Specifically, metadata, notably location records, device identifiers, and logs of use, tend to have a decisive evidentiary quality, despite the fact that they are usually not produced with any intent to do so.[26] Simultaneously, there is the concern of the technical complexity of digital forensics. The scholars of jurisprudence warn that in the process of data extraction, data maintenance, and data interpretation, there are no errors, limitations in the methodology, or subjective bias. Forensic methodology can create a blind spot that hides the shortcomings of analysis, and thus influences the accuracy of evidence and, ultimately, the justice of the criminal process.[27]

[25] Sandi YudhaPrayoga, 'The Criminal Justice System and Technology in the Digital Age' (2024) *Edunity* 551–552
[26] Stoykova, (n 4) 2216–2217
[27] Andrea Roth, 'Machine Testimony' (2017) 126 YLJ 1972

One major statutory reaction to these fears may be found in the Bharatiya Nagarik Suraksha Sanhita, especially in Section 176. Section 176 requires the use of audio-video records in the search and seizure operation, including the forensic procedures, and, by extension, provides an important dimension of transparency and accountability to the forensic process[28].

This is a technological protection that has two purposes. First, it enhances the honesty of the evidentiary process because it reduces the chances of tampering, fabrication, and procedural anomalies at the crime scene. Second, more significantly, it redefines the purpose of technology in the criminal justice system, not as a tool of state surveillance but as a tool of defence of the victims. The recording of the forensic procedure through audio-video recording will ensure that the collection and handling of evidence is performed in a way that will not alter the authenticity of the victim's case and thus will bring confidence in the investigative process.[29]

Section 176 BNSS is thus a paradigm shift in this manner. It shows how the technological integration, when controlled, can be used to strengthen the procedural fairness and, at the same time, empower the victims. It helps to build a more balanced and victim-oriented notion of justice under Article 21 that is more in balance between the rights of the accused and the dignity and participatory rights of the victim, and which promotes transparency in forensic practices as well as preservation of the integrity of evidence. Owing to it, the digital evidence may be given disproportionate probative weight, and it may influence the procedural fairness without undergoing stringent scrutiny.

3.5. Emerging AI-Based Surveillance Tools

The use of AI in surveillance has provided a new aspect of surveillance with the aid of predictive policing algorithms, facial recognition systems, and automated risk assessment models. These technologies rely on large datasets to identify correlations and forecast criminal activity. While they are promoted as enhancing objectivity and efficiency, academic literature emphasises that algorithmic systems often operate as opaque "black boxes," making it difficult for courts and accused persons to understand or challenge their outputs. The reliance on probabilistic predictions rather than concrete evidence represents a significant departure from traditional investigative logic.

[28] Bharatiya Nagarik Suraksha Sanhita 2023, s 176
[29] *Id*

3.6. Objectives Claimed by the State

States commonly justify the adoption of surveillance technologies by invoking objectives such as investigative efficiency, crime prevention, and national security. Technological tools are presented as necessary responses to complex and transnational forms of crime, particularly in an era of digital communication. However, legal commentary stresses that these objectives must be balanced against constitutional commitments to liberty and procedural justice. The framing of surveillance as an administrative necessity risks marginalising rights-based concerns and weakening judicial oversight.[30]

3.7. From Traditional Investigation to Data-Driven Policing

The cumulative effect of these developments reflects a broader shift from reactive, offence-based investigations to proactive, data-driven policing models. Modern criminal justice is becoming more based on the accumulation of information, constant surveillance, and predictive analysis as opposed to case-specific investigation. According to scholars, this has changed the criminal procedure towards managerial efficiency instead of adversarial fairness. This therefore requires that the growth of technological surveillance requires a review of the current legal regimes to ensure that innovation does not undermine pre-established rules of justice and due process.

4. Impact of Technological Surveillance on Criminal Procedure

4.1. Transformation of Investigation Processes

Surveillance by technology has radically changed the character and direction of criminal investigations. Continuous collection of data and automated monitoring, instead of traditional methods of investigations that were based on witness testimony, physical searches and post-offence inquiry, are becoming more supplementary or substitutes. The investigations of crimes can no longer be limited to the response to a particular crime, but rather they tend to work based on proactive and intelligence-driven models, where the primary focus is on the accumulation of information and not on the particular suspicion of a case. Scholars note that this

[30] Sandi YudhaPrayoga, 'The Criminal Justice System and Technology in the Digital Age' (2024) *Edunity* 552–553

transformation has changed the logic behind criminal procedure to no longer be reactive adjudication but rather preventative and risk-based enforcement.[31]

Such a transformation raises concerns regarding the compatibility of surveillance-driven investigations with established procedural safeguards.

4.2. Digital Evidence Collection, Storage and Use

The growth of technological surveillance has led to a new amount of digital evidence entering criminal proceedings. Law enforcement agencies have become regular in their gathering of information on mobile devices, communication services, cloud service providers, and digital infrastructures. Such information can be retained over a long time and used in numerous studies; thus, it is not clear which is the evidence collected to investigate a particular crime and which is the data that can be used in new studies. The study of law emphasises that the volume and permanence of digital storage open the risk of abuse, secondary exploitation, and creep of functions, especially where there are no clear statutory boundaries.[32] The factual worth of online content is often presupposed as opposed to being evaluated, regardless of the technical nature of its retrieval and deciphering.

5. Judicial Pronouncement and Evolving Standard

The judicial reactions to technological surveillance have been an ongoing effort at finding some balance between state interests in efficient enforcement of its laws and constitutional and human rights promises of fair trial and due process. The increased recognition by courts has been that the technological changes, despite not necessarily being unlawful, require greater attention because they are intrusive and may upset the fairness of the process. Instead of taking a technology-neutral position, judicial rhetoric has progressively been shifting towards the right-sensitive model of judicial reasoning, focused on proportionality, legality, and accountability in surveillance activities.

Courts at the constitutional level have always acknowledged procedural fairness to be a fundamental part of the right to live and personal liberty. In *Maneka Gandhi v Union of India,* the Supreme Court of India broadened the interpretation of the term procedure established by

[31] Andrew Ashworth and Lucia Zedner, 'Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure and Sanctions' (2008) 2 CLP 21

[32] Stephen Mason and Daniel Seng, *Electronic Evidence* (4thedn., Institute of Advanced Legal Studies 2017) para 2.15

law to demand that this procedure be fair, just and reasonable, thus establishing the basis of judicial exercise in investigative methods that have an impact on individual freedom.[33] This interpretative method has played a key role in evaluating surveillance policies that are working at the pre-trial phase, where procedural protections are most vulnerable but have the most impact.

The involvement of the judiciary in surveillance has also developed, with privacy being acknowledged as a constitutionally guaranteed interest. The Supreme Court considered that privacy was inherent in the dignity and liberty, and Interception by the state would be subject to the tests of legality, necessity and proportionality. [34] The case was not directly caused by criminal surveillance, but its principles have an important implication in criminal procedure, especially in determining the legality of electronic eavesdropping, data gathering, and continuous surveillance. Courts are gaining a requirement to determine whether surveillance practices are limited and have sufficient procedures to safeguard them.

The international jurisprudence has also impacted the changing standards. The European Court of Human Rights has made it very clear several times that fairness according to Article 6 of the European Convention on Human Rights should be evaluated through considering proceedings as a whole. In Deweer v Belgium, the Court pointed out that even where the efficiency criteria are used, no state practice can be coercive or imbalanced to the detriment of procedural fairness. This broad-based strategy has helped the courts to review evidence obtained through surveillance not only at the admissibility test but also in the context of its overall effect on the sanctity of the criminal process.[35]

The response of judicial action in the formation of these developments is still meek and, in the majority of cases, pathetic. Post-facto assessment of surveillance practices by the courts is likely to place emphasis on the admissibility, but not to challenge the structural inequalities that are instituted due to the technological asymmetry. It is suggested in the literature that the reluctance of the judiciary to get too much involved in the finer details of surveillance acts as a disincentive to the proper checks and balances, particularly where the judge is himself heavily depending on the revelations made by the executive or where he or she has resorted to the

[33] *Maneka Gandhi v Union of India* AIR 1978 SC 597
[34] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[35] *Deweer v Belgium* (1980) 2 EHRR 439

expert eye which has been carefully courted by the prosecution.[36] Thus, the new norms have not fully addressed the matters of transparency, equal armament and heavy defence participation.

Recent jurisprudence does indicate a slow, but undoubted, turn towards standards based upon principle, based upon proportionality, necessity and upon procedural protections. Courts have become more aware that the efficiency of technology can not be used as an excuse to weaken the guarantees of the fair trial and that surveillance programs should work within specific legal boundaries. This changing picture of judicial treatment highlights the necessity of a more systematic approach to the doctrine of the law, an approach that would bring together technological innovations and the basic tenets of criminal justice, including fairness, accountability, and due process.

Notably, this change is not limited to the regulation of state power but also to extending victim-oriented safeguards to the justice system. In Mallikarjun Kodagali v State of Karnataka, the Supreme Court firmly accepted the position of victims having a substantive and independent right to appeal against acquittal, and therefore places them on a more equal standing with the accused, who already has a right to appeal against conviction. The Court underlined that victims should not be marginalised by the criminal justice system, and their rights to participate in the justice process are vital elements of a just and complete justice process.[37]

The doctrine has been strengthened further by the recent case of Syed Shahnawaz Ali v State of MP, which made it clear that the right of the victim to seek justice, including the right to seek revision or appeal, does not cease to exist with death. Rather, these rights may be pursued by the legal counsel of the victim, therefore, allowing the pursuit of justice not to be cut short.[38]

When combined, the decisions do create a strong kind of protection mechanism in the criminal justice system. They represent a doctrinal development in which the victim's rights are no longer considered as incidental but as substantive and enforceable under Article 21. These developments, when taken together with the mounting judicial pressure to regulate technological surveillance by means of proportionality and necessity, should lead toward a more moderate and integrated system, one that manages to restrain the ambitions of the state,

[36] Bart H M Custers, 'A Fair Trial in Complex Technology Cases: Why Courts and Judges Need a Basic Understanding of Complex Technologies' (2024) 52 *Computer Law & Security Review* 105935
[37] *Mallikarjun Kodagali v State of Karnataka* (2019) 2 SCC 752
[38] *Syed Shahnawaz Ali v State of Madhya Pradesh* (2025) SCC OnLine SC (Dec 2025)

protects the interests of the accused, and establishes the timeless participatory rights of the victims.

6. Procedural Challenges Arising Due to Surveillance Practice

6.1. Lack of Transparency

Among the procedural issues that may have the greatest impact on the technological surveillance practice is the loss of transparency. Surveillance technologies are usually covert in nature, and the targeted individuals may not even know the presence of monitoring, as well as the scope of the data being collected. The semi-transparency of digital systems, especially those that employ automated analytics or proprietary software, prevents the effective examination of courts and defence attorneys. According to academic examination, this kind of insufficient transparency impedes procedural fairness because the accused is not able to know how the evidence was produced, and whether such evidence was acquired in accordance with the law.[39]

6.2. Executive Discretion

The growing use of technology surveillance has greatly broadened executive discretion in investigating a crime. In many cases, administrative agencies dictate whom to monitor, what type of data to gather, and how long such data should be stored--in many cases without any judicial review. This accumulation of power is highly alarming because researchers have warned of a situation where excessive reliance on executive discretion will turn surveillance into a tool of intrusion and unaccountability, making the criminal procedure less effective as a check and balance mechanism against the abuses of state power.

This issue is especially acute when regarded through the prism of the Digital Personal Data Protection Act 2023. Section 17(1)(c) of the Act does not impose on law enforcement agencies any data protection requirements when handling personal data with a view to investigation, detection or prosecution of crime. Although this exemption is designed to help police officers effectively conduct their work, it also poses a constitutional dilemma: the weakening of privacy protections at the point when accused and victims are the most at risk.[40]

[39] Bart H M Custers, 'A Fair Trial in Complex Technology Cases: Why Courts and Judges Need a Basic Understanding of Complex Technologies' (2024) 52 CLSR 105935
[40] Digital Personal Data Protection Act 2023, s 17(1)(c)

Constitutionally speaking, under Article 21, this blanket exemption has brought about the vulnerability to secondary victimization especially when it comes to sensitive cases like sexual offences. Personal online information of victims, including personal messages or photos, health records, etc., can be accessed, processed or even kept without proper procedures, safeguards and accountability. Lack of stringent control enhances the chances of misuse, breach of confidentiality, or reputational damage, thus worsening the trauma experienced by the victim.[41]

The unrestrained growth of surveillance authority in this regard not only raises the issue of the rights of the accused but also threatens the dignity and privacy of victims. Constitutional study should thus highlight the necessity to work out the compatibility of such statutory exemptions with the notions of proportionality, necessity, and procedural fairness. This involves creating strong safeguards, including limited purpose usage, data minimisation, protocols to handle data safely, and independent supervision, to make sure that the efficiency of investigation does not result in violating the basic rights.

Finally, although surveillance technologies may lead to the improvement of criminal investigations, their validity is determined by the presence of significant checks on the executive authority. In the absence of these safeguards, the criminal justice system runs a risk of losing the reason why it was formed: it is not only to detect and punish crime in a way that does not violate the dignity, privacy and rights of all stakeholders and the victims in particular.

6.3. Lack of Previous Judicial Supervision

The question that has been brought up repeatedly in the literature is the lack, or watering down, of previous judicial control over the process of surveillance measures authorisation. In most cases, surveillance is done based on sweeping statutory requirements or based on emergency grounds and judicial review is done when evidence is already gathered. This ex post facto control is not necessarily enough to avoid the infringement of rights because unlawfully acquired data might already have changed the direction of the investigation. According to jurisprudential commentary, procedural legitimacy and arbitrary intrusion can only be avoided by insisting that prior judicial authorisation is necessary.[42]

[41] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[42] *Deweer v Belgium* (1980) 2 EHRR 439

6.4. Admissibility and Authenticity of Electronically Obtained Evidence.

The increasing use of electronically obtained evidence has largely threatened the conventional guidelines of admissibility and authenticity. In contrast to the traditional evidence type, digital evidence is born digital, and a court has to contend with sophisticated forensic procedures. Although this evidence may be very probative, it is also prone to extraction errors, manipulation dangers and interpretation bias. The issue of chain of custody, data integrity, and methodological reliability are areas where the concerns are not adequately reviewed in the courtrooms, which contributes to inconsistency in the evaluation of digital evidence and its use in making a judicial decision.[43]

The Bharatiya Sakshya Adhiniyam 2023 has brought a paradigm change in this field. Section 63 of BSA has revised the admissibility regime of the electronic evidence, which supersedes the previous one and eases the procedural conditions. More importantly, Section 57 of the Act expressly acknowledges electronic records as primary evidence where they are brought reasonably into existence out of lawful custody.[44] This is one of the most far-reaching evidentiary changes in the last century that essentially changes the attitude of courts toward and their approach to digital material.

This way, by making electronic records count as primary evidence, the law will minimise procedural obstacles that would otherwise slow down trials and make it harder to prove. The constitutional implications of this change are direct: it allows the adjudication process to proceed faster and, thus, provides the victim with the right of speedy justice as stipulated by Article 21. Meanwhile, it imposes a heavier burden on the courts with the duty of conducting a stricter check on the validity and reliability of such evidence, as it is prone to technical manipulation.

Therefore, though the BSA 2023 simplifies the admissibility of digital evidence and enhances the efficiency of criminal trials, it also means that there should be a uniform method of judicial review of reliability. The key is a middle ground that makes use of technology in order to deliver justice to victims promptly but in a manner that does not compromise on the fairness and accuracy on which the criminal justice system is founded.

[43] Andrea Roth, 'Machine Testimony' (2017) 126 YLJ 1972
[44] Bharatiya Sakshya Adhiniyam 2023, s 57 & 63

6.5. Effect on the Right of the Accused to object to Prosecution Evidence.

Technological surveillance has a great influence on the ability of the accused to dispute the prosecution's evidence. The structural disadvantage is because the technical intricacy of digital systems and the lack of access to the underlying algorithms or source data, puts the defence at a structural disadvantage. Legal commentators believe that in cases where evidence is created using opaque technological procedures, the right to successfully challenge its trustworthiness becomes an illusion.[45] This lack of balance is especially severe in situations where it comes to artificial intelligence or any other tools of automated decision-making, where the defence might not only be untechnical but also have no avenue of disclosure through the courts.

6.6. Procedural balance between Defence and Prosecution.

The sum total of surveillance technologies has helped to create an imbalance in the procedures between prosecution and defence. Whilst prosecution advantages themselves with massive technological capabilities, expert experience, and access to surveillance information, the defence usually has a hard time locating meaningful disclosure or external validation. According to scholars, this imbalance is a violation of the principle of equal arms, which is the core of equal criminal procedure.[46] In the absence of procedural changes to match the level of technological surveillance, there is a danger that structural inequalities will become embedded in the surveillance and are likely to undermine the fairness and legitimacy of criminal trials.

7. Fair Trial Issues that Arise Out of the Surveillance Practices

The growing application of technological surveillance has posed significant issues to the criminal justice system, particularly concerning the right to a fair trial. Surveillance equipment is usually popularised as an impartial way of stopping and identifying crime. Practically, however, their application has modified the relations between the power of the state and individual rights. Nowadays, a great part of criminal cases is formed at the very investigation level. Surveillance dictates how one becomes a suspect, the collection of evidence, and the

[45] Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) 49 CLSR 105801

[46] Christophe Champod and Joëlle Vuille, 'Scientific Evidence in Europe: Admissibility, Evaluation and Equality of Arms' (2011) 9 ICE 1

course of a case. This casts serious questions on fundamental principles like presumption of innocence, confidentiality, equality of arms and due process.

7.1. Presumption of Innocence

The presumption of innocence assumes that everybody is innocent until they are found guilty in a lawful process. Nevertheless, predictive analytics and data trends have become highly dependable in surveillance-based policing, which allows monitoring of a crime before it is committed. This move toward evidence-based suspicion to risk-based profiling is dangerous to negate this fundamental tenet of criminal law. The most important protection is the Bharatiya Nagarik Suraksha Sanhita,2023, in which Section 360 provides the right of the victim to be heard before prosecution withdrawal, which promotes participatory justice as well as balancing technological excess with constitutional fairness in Article 21.

Bias is also a serious threat. Most surveillance systems will be based on previous law enforcement records. In case such data is biased socially or economically, the system might replicate and enhance these trends.[47] Some groups might be observed more, which results in over-policing. This undermines the presumption of innocence because it is aimed at making statistical assumptions that people are potential criminals and not on the basis of their behaviour.

7.2. Right to Privacy and Fair Trial

Privacy is a significant factor towards getting a fair trial, particularly before the court trial. The surveillance usually encompasses checking of personal communications and location information, as well as day-to-day activities. In most other instances, people do not know the extent of information being gathered against them. The intrusion of this kind, in the absence of strict control, has been repeatedly indicated by legal scholars as potentially undermining the fairness of subsequent trials.[48]

There are also difficulties associated with illegal or excessive surveillance. Although the admissibility may be studied later by courts, it might be too late. Obtained illegal information

[47] P Neyroud and E Disley, 'Technology and Policing: Implications for Fairness and Legitimacy' (2008) 2 *Policing* 226

[48] Bart H M Custers, 'A Fair Trial in Complex Technology Cases: Why Courts and Judges Need a Basic Understanding of Complex Technologies' (2024) 52 *Computer Law & Security Review* 105935

may affect investigations, indictments, and the discovery of evidence. It is true that in many instances, it is too late to rectify the damage done during the initial stages after execution.[49]

7.3. Equality of Arms

Equality of arms means that fair opportunity of both parties in a criminal case have a fair opportunity to put forward their cases. Surveillance upset this fact by providing the prosecution with more information and technical resources. Surveillance data and systems are controlled by law enforcement, whereas the defence relies on limited disclosure.[50]

This is further exacerbated by the technicality of the surveillance tools. Defence attorneys do not normally have access to the inner-workings of digital systems. The full comprehension of these technologies may also be a problem for courts. This puts the defence at a disadvantaged bargain and the trial is at risk of becoming inequitable in application.

7.4. Due Process and Judicial Review.

Due process demands that the surveillance should be under strict control and monitored. Nevertheless, most surveillance habits are weak in authorisation procedures. The judicial approval is sometimes not made based on much information, and there is little time to question it. This grants laxity on the control to a mere formality as opposed to a genuine protection.

The other significant issue is that there was no prior judicial approval. Monitoring has already been conducted, and it has not stopped abuse. Legal experts emphasise that in order to have meaningful protection of the right to fair trial, it is essential that the process of surveillance is subject to judicial oversight prior to commencement of the surveillance process, particularly where surveillance methodologies are very invasive.[51] In general, criminal justice based on surveillance poses enormous threats to fair trials. It transfers authority to the state, undermines protection, and prioritises efficiency in justice. To overcome these issues, it is necessary to enforce more strict legal regulation of the matter and reinstate the principles of fair trial through a trial at any level of the criminal process.

[49] Erin Murphy, 'The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence' (2007) 95 CLR 721
[50] Christophe Champod and Joëlle Vuille, 'Scientific Evidence in Europe: Admissibility, Evaluation and Equality of Arms' (2011) 9 ICE 1
[51] Andrew Ashworth and Lucia Zedner, 'Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure and Sanctions' (2008) 2 CLP 21

8. Reform Necessity and Safeguards

The growing use of technological surveillance in criminal justice systems has revealed some loopholes in the available pieces of law and procedures. Although the surveillance technologies are efficient and expected to control crime better, their unregulated use threatens to compromise fair trial provisions. Comprehensive changes that include the balance between the effectiveness of investigations and the constitutional and human rights are therefore badly needed. These reforms should have legislative, procedural and institutional functions.

8.1. Legislative Reforms

Among the key conditions, such as the establishment of a definite and elaborate policy of the application of surveillance technologies, can be listed. The existing laws are typically fractured, technologically primitive, or vague, giving excessive flexibility to the executive authority. The legal scholarship is that the surveillance authority should be clearly defined in the law, the scope and purpose of it, the time frames of the surveillance and the admissible methods of gathering the data.[52] The presence of a clear statutory framework would enhance the predictability of law and prevent naturalisation of invasive surveillance practice under the guise of, in the name of, the public interest of security.

The use of powerful accountability tools is also important. Documentation, review, and reporting of such activities should also be a law requirement to make sure that it is not in the scenario of abusing surveillance or in a manner that is not the reason it was first instituted. Without these provisions, surveillance would tend to remain a concretely constant form of governance as opposed to an investigative tool of extraordinary nature.[53]

8.2. Procedural Reforms

The procedural safeguards play a crucial role in the process of translating the aim of the law into the protection of the fair trial rights. The practice of intrusive surveillance should be open to prior judicial authorisation so as to remind the security officials that they have to be based on necessity and relevance and not administrative convenience. Researchers have always held

[52] Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) 49 CLSR 105801

[53] Andrew Ashworth and Lucia Zedner, 'Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure and Sanctions' (2008) 2 CLP 21

that post-facto review is an inappropriate alternative because it cannot stop rights abuses at the earliest stage.[54]

Simultaneously, there is still a critical normative vacuity in the achievement of victim rights in this procedural system. Although the Bharatiya Nagarik Suraksha Sanhita has some valuable guarantees, including Section 193 (registration of information) and Section 230 (supply of documents), victims are more likely to need institutional support to effectively exercise their rights.

To deal with this, the role of the District Victim and Witness Protection Officer (DVWPOs) needs to be formalised as the special body to help the victims during investigation and pre-trial procedures. Further, legal provision of compulsory state-funded legal assistance must also be enhanced so as to make sure that victims are effectively informed, represented and empowered to participate in the procedural machinery. These reforms would not only formalise the current statutory protections but would also fill the gap between legal eligibility and reality, access to justice, which would further promote a more robust and victim-focused constitutional structure in 2026.

The other relevant procedural safeguard is the disclosure to the defence. To render the right to a fair trial meaningful, the technicality, amount and manner of the surveillance exercised on an accused should be provided to him or her. Selective or partial disclosure has a mass of ill consequences to the defence power of the attempt to challenge the lawfulness and trustworthiness of the pieces of evidence.[55] The procedural reform should, therefore, meet the timely and sufficient disclosure, with the exceptions being on a narrow focus.

There should be independent overseers also. The compliance with the laws of surveillance can be checked, the misuse can be checked, and remedial recommendations can be made through these bodies, the action of which is independent of the law-enforcing agencies. This is a result of an external audit that results in increased trust among the citizens and renders the criminal justice system's surveillance practices legitimate.[56]

---

[54] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

[55] Christophe Champod and Joëlle Vuille, 'Scientific Evidence in Europe: Admissibility, Evaluation and Equality of Arms' (2011) 9 ICE 1

[56] Neyroud and E Disley, 'Technology and Policing: Implications for Fairness and Legitimacy' (2008) 2 *Policing* 226

8.3. Capacity Building and Strengthening of the Institution

The legislative reform has to be followed by long-term capacity building. Cases involving sophisticated technologies, digital evidence, and robot decision-making technologies have to be tried more and more by judges. This means that relevant oversight and sound decision-making cannot occur without judicial training programmes that are geared towards technological literacy.[57]

On the same note, defence lawyers should have access to technical knowledge, be it expert services funded by the state or institutional support systems. In the absence of it, the balance of criminal proceedings in an adversarial scheme is still lopsided towards the prosecution. By academic commentary, procedural equality cannot be realised alone based on formal rights, but rather must be accompanied by practical ability to make any action out of this right practical.[58]

All these reforms are important reminders of why technological surveillance should be institutionalised through the prism of a rights-oriented criminal justice system. The clarity of legislation, institutional capacity, and procedural control are necessary in order to make sure that the developments in technology reinforce instead of undermine the principles of fair trial and due process.

9. CONCLUSION

One of the most prominent elements of contemporary criminal justice has turned out to be technological surveillance. Investigative activities have gained a great deal of speed in the last few years due to the use of digital tools, which in most cases have resulted in faster and better cases. Surveillance technologies have become a common and regular method for police departments to profile suspects, gather data, and develop criminal evidence. Although there has been an increase in investigative capacity of these tools, there has also been a concern about their increasing use, which has raised grave concerns in the criminal procedure.

The most disturbing problem is how surveillance can influence a case way before it is even heard in court. The application of monitoring technologies affects the way people form

[57] Bart H M Custers, 'A Fair Trial in Complex Technology Cases: Why Courts and Judges Need a Basic Understanding of Complex Technologies' (2024) 52 CLSR 105935
[58] Erin Murphy, 'The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence' (2007) 95 CLR 721

suspicions, accumulate evidence and are carried out by prosecutors. Consequently, people will be the subject of suspicion, mostly due to the patterns in the data or automated surveillance, and not tangible and evident facts. The presumption of innocence, which is a fact of just criminal proceedings, is directly challenged by this development.

Moreover, most surveillance systems are very complicated and technically obscure. Lack of proper information regarding the operations of such technologies and the process of data creation and analysis leaves the real challenges in appealing against the evidence presented against the defendants. Such a transparency deficiency puts the defence at a structural disadvantage compared to the resources and technical capabilities of the State. This disproportion poses risks to the principle of equality of arms, which is central to promoting legitimacy and fair play in criminal trials.

These are some of the concerns that courts have started paying attention to. The rulings of courts are tending to invoke the provisions of legality, necessity and proportionality in determining surveillance-based investigations. Nevertheless, it is usually judicial oversight that takes place at a time when the surveillance has already been carried out. Courts, on most occasions, are requested to evaluate evidence that has already been gathered and not stop dubious practices beforehand.

Without a clear legal system, strong checks and mechanisms, and properly equipped institutions, surveillance can be just a tool of routine investigation and not an exceptional resort. Such normalisation can remove procedural safeguards over time that are vital to a justice system that is fair.

In conclusion, the digital age has subjected the criminal justice system to serious scrutiny, and it has been noted that there must be a balance between technological progress and the safety of fundamental rights. Justice should not be replaced by technology. A surveillance practice has to be carried out in obedience to a well-distributed law and should be guided by procedural perception favouring level and just procedure as well as due methods. It is only in such instances that the right to a fair trial can be used successfully in an ever-more-digitised criminal justice system.

***