Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

Smart Witness Protection Mechanisms and Artificial Intelligence: Legal and Regulatory Challenges in India

Akansha Chandela[1]*, Dr. Apala Vatsa[1]
[1]Manav Rachna University, Faridabad, Haryana, India

Abstract

Witness protection has emerged as a critical dimension of criminal justice reform in India, particularly considering persistent concerns regarding intimidation, coercion, hostility, and retaliatory harm faced by witnesses in serious criminal trials. In parallel, the rapid diffusion of artificial intelligence (AI), data-driven governance, and digital public infrastructure has opened new possibilities for strengthening state capacity, improving case management, and enabling more responsive protective frameworks. This paper situates witness protection within the broader interdisciplinary discourse on AI-enabled governance, legal-regulatory reform, and business analytics, with specific emphasis on India's criminal justice system. It argues that "smart" witness protection mechanisms—understood as digitally supported, risk-sensitive, and administratively coordinated systems—may enhance the efficiency, precision, and scalability of witness safeguarding, but only if embedded within robust legal controls, procedural safeguards, institutional accountability, and privacy-sensitive governance. The paper develops a conceptual analysis of the opportunities and constraints associated with AI-assisted witness protection in India, including risk assessment, threat monitoring, secure case allocation, inter-agency coordination, anonymization, relocation planning, and compliance tracking. It also examines the legal and regulatory challenges that accompany the use of AI in this domain, such as bias, opacity, data protection, due process, evidentiary fairness, cybersecurity, and uneven institutional capacity. The core argument is that technological innovation cannot substitute for legal design; rather, AI should be treated as an enabling instrument within a rights-based, constitutionally grounded, and institutionally auditable witness protection regime. The paper concludes by proposing a policy architecture for India that aligns technological tools with legal accountability, judicial oversight, and victim-witness centric criminal justice reform.

Keywords: *legal reform; criminal justice; data-driven governance; regulatory governance; smart justice systems*

1. Introduction

The credibility of criminal adjudication depends not only on investigative competence and prosecutorial diligence but also on the ability of the justice system to secure truthful testimony without exposing witnesses to intimidation or harm.[1] In many legal systems, and particularly in jurisdictions confronting high case backlogs and uneven enforcement capacity, witnesses remain among the most vulnerable actors in criminal proceedings.[2] Their vulnerability can distort evidence, weaken prosecutions, and undermine public confidence in the rule of law. Witness protection, therefore, is not a peripheral procedural concern; it is foundational to the integrity of criminal trials and the delivery of complete justice.[3]

In India, the challenge of witness protection is especially significant because criminal trials often involve social hierarchies, local power structures, resource asymmetries, and risks of retaliation.[4] These realities generate a persistent gap between formal rights and effective courtroom participation. At the same time, India is witnessing the expansion of digital governance, algorithmic decision support, and AI-enabled public administration across

[1] Ratanlal and Dhirajlal, *The Code of Criminal Procedure* (23rd edn, LexisNexis 2020) 12.
[2] Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006) para 1.3.
[3] *Zahira Habibullah Sheikh v State of Gujarat* (2004) 4 SCC 158.
[4] Ranbir Singh, 'Witness Protection in India: Problems and Prospects' (2015) 57(3) Journal of the Indian Law Institute 421.

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

sectors.[5] These developments invite a renewed inquiry into whether technologically mediated systems can improve witness safety, case coordination, and institutional responsiveness. The question is not merely technical; it is fundamentally normative and legal. Can AI assist in building a more secure and efficient witness protection framework without compromising fairness, privacy, and accountability?

This paper addresses that question by framing witness protection as an area where AI and data-driven governance may support legal reform in India. Although the paper is anchored in the PhD thesis theme of evolving a right legal framework for witness protection towards rendering complete justice in criminal trials in India, it is written for an economic sciences journal special issue on AI and data-driven strategies in marketing, economics, and business analytics. Accordingly, the analysis also highlights the governance and administrative dimensions of witness protection, including resource allocation, operational efficiency, risk modelling, institutional coordination, and decision support. These themes are relevant to business analytics and public-sector analytics because witness protection systems must manage scarce resources, prioritize threats, and maintain secure information flows under conditions of uncertainty.[6]

The central claim advanced here is that "smart witness protection" should be understood as a governance model rather than merely a technological toolkit. AI may assist in identifying risk patterns, automating alerts, supporting secure communication, and optimizing protective interventions. Yet such capabilities require a legal framework that defines permissible uses, establishes oversight, prevents misuse, and preserves the procedural rights of accused persons and witnesses alike.[7] In the absence of such a framework, AI could amplify existing vulnerabilities by reproducing bias, generating false confidence, or exposing sensitive information. Therefore, the proper legal response is neither technological enthusiasm nor technological rejection, but calibrated regulation.[8]

The paper makes five contributions. First, it conceptually situates witness protection within AI-enabled governance and data-driven public administration. Second, it identifies the principal operational use cases through which AI might improve witness protection in India. Third, it analyses legal and regulatory tensions, particularly in relation to privacy, due process, equality, and accountability. Fourth, it proposes a reform-oriented policy architecture for smart witness protection. Finally, it demonstrates why witness protection should be treated as a critical component of criminal justice efficiency and institutional trust.

2. Problem Statement

The problem addressed in this paper is the mismatch between the normative importance of witness protection and the practical inadequacy of existing institutional responses in India. In many criminal cases, witnesses face intimidation, delay, relocation challenges, surveillance risks, social coercion, and uncertainty about confidentiality.[9] These problems are aggravated by fragmented coordination among police, prosecution, courts, and correctional authorities.[10] The result is a system in which witness protection is often reactive, under-resourced, and dependent on ad hoc administrative discretion rather than structured, data-informed governance.

A second layer of the problem concerns the governance of information. Witness protection is an information-intensive domain. Authorities must collect, store, process, and transmit highly sensitive data about identity, location, threat level, and logistical arrangements. Traditional paper-based or

[5] Ministry of Electronics and Information Technology, *National Strategy for Artificial Intelligence* (NITI Aayog 2018) 8–12.
[6] Christopher Hood and Helen Margetts, *The Tools of Government in the Digital Age* (Palgrave Macmillan 2007) 67.
[7] *Justice K S Puttaswamy v Union of India* (2017) 10 SCC 1.
[8] Frank Pasquale, *The Black Box Society* (Harvard University Press 2015) 18–20.
[9] Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006) paras 2.1–2.6.
[10] Witness Protection Scheme 2018, approved in *Mahender Chawla v Union of India* (2019) 14 SCC 615.

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

fragmented digital systems are poorly suited to this task. They increase the risk of leakage, delay, duplication, and inconsistent decision-making.[11] At the same time, the growing adoption of AI in public administration creates both opportunities and dangers. AI could support pattern recognition and service delivery, but it may also enable intrusive surveillance, opaque scoring, and automated decisions that are difficult to contest.[12]

A third layer of the problem is legal. Indian criminal procedure and constitutional principles require fairness, equality, and the protection of life and personal liberty.[13] Any witness protection architecture must therefore reconcile two imperatives: protecting the witness and preserving due process for the accused. This is particularly important when protective measures affect anonymity, disclosure obligations, in-camera procedures, access to records, or the admissibility and credibility of testimony.[14] The legal framework must also address data protection, cybersecurity, inter-agency authority, record retention, auditability, and remedies for misuse.[15]

Accordingly, the key problem is not simply whether AI can be used in witness protection, but how a legally robust and institutionally accountable AI-assisted witness protection regime can be designed for India. This requires a multidimensional analysis spanning law, governance, analytics, and public administration.

3. Conceptual Framework: Smart Witness Protection as Data-Driven Governance

"Smart witness protection" refers to a system in which protective decisions and administrative processes are supported by digital infrastructure, analytics, and AI-enabled decision support. The term "smart" should not be read as implying full automation. Rather, it denotes the use of structured data, secure platforms, and analytic tools to improve coordination, timeliness, and risk sensitivity in witness safeguarding.

From a governance perspective, smart witness protection can be understood through four interrelated functions:

1. **Risk identification and prioritization** - AI systems may assist in identifying cases with higher intimidation risk by analysing structured indicators such as case type, threat reports, prior incidents, geographic vulnerability, or patterns of witness withdrawal. In practical terms, such analytics can help authorities move from intuition-driven responses to more systematic triage, especially where the number of potentially vulnerable witnesses exceeds the immediate capacity of protection agencies. A structured risk model can also reveal recurring warning signs that may otherwise be missed in fragmented case files.
2. **Protective planning and resource allocation** - Administrative analytics can help authorities allocate limited protective resources more effectively across cases, distinguishing between high, medium, and low risk categories and matching them to appropriate interventions. This is especially important in a resource-constrained system, where protective measures such as escort arrangements, relocation support, safe transport, secure lodging, and communication controls cannot be extended uniformly to all witnesses at all times. Analytics can therefore support proportionality by linking risk level to the intensity of the response.
3. **Secure case management and communication** - Digital platforms may support controlled sharing of information among authorized actors, reducing leakage and improving coordination between police, prosecutors, courts, and witness protection units. In a witness protection setting, the quality

[11] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 95–97.
[12] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 Georgetown Law Journal 1147.
[13] Constitution of India, arts 14 and 21.
[14] *State of Punjab v Gurmit Singh* (1996) 2 SCC 384.
[15] Digital Personal Data Protection Act 2023.

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

of communication is not simply a matter of administrative convenience; it is a determinant of safety. Secure case management systems can create compartmentalized access, time-stamped actions, and encrypted records, thereby reducing opportunities for unauthorized disclosure while also making internal coordination more reliable.

4. **Monitoring, compliance, and auditability** - Dashboards and logging tools can track whether protection measures are implemented on time, whether alerts are acted upon, and whether the system respects procedural boundaries. This monitoring function is central to institutional accountability because witness protection often fails not at the stage of policy formulation but at the stage of execution. Audit trails, compliance dashboards, and escalation triggers can help ensure that protective directions are not merely issued but meaningfully implemented.

This framework is conceptually aligned with contemporary data-driven governance, where public institutions increasingly rely on analytics to improve efficiency, service delivery, and oversight.[16] In the context of witness protection, such analytics may function as a form of operational intelligence. However, the logic of public administration cannot be imported uncritically into criminal justice. Witness protection implicates fundamental rights, evidentiary fairness, and the integrity of adversarial procedure. For this reason, the design of smart systems must be guided by legal principles rather than by efficiency alone.[17]

In economic sciences terms, witness protection can be viewed as a public good with positive externalities: when witnesses are protected, the criminal justice system becomes more credible, deterrence improves, and enforcement outcomes become more reliable. Yet because the benefits are diffuse while the costs are immediate, witness protection is often underprovided. Data-driven governance and AI may reduce transaction costs, improve targeting, and enhance institutional capacity, but only if the underlying legal regime permits reliable data use and imposes clear responsibilities.[18]

4. Literature-Informed Argumentation

The broader interdisciplinary literature on AI in governance suggests that algorithmic tools can improve prediction, coordination, and operational efficiency while also intensifying concerns about opacity, bias, and accountability.[19] In public administration, data analytics is often justified as a means of improving evidence-based decision-making, especially where resources are scarce and demand exceeds administrative capacity.[20] These ideas are relevant to witness protection because the domain requires continuous risk assessment, rapid response, and secure handling of sensitive information.

In legal scholarship, witness protection is commonly treated as a procedural safeguard necessary to preserve the truth-seeking function of criminal trials.[21] The literature emphasizes that witness intimidation can distort testimony and reduce the effectiveness of prosecution, particularly where organized violence, local coercion, or institutional weakness are present.[22] It also highlights the need for protective measures that are not merely symbolic but operationally credible.

[16] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013) 96.
[17] Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (New York University Press 2017) 42–45.
[18] Douglass C North, *Institutions, Institutional Change and Economic Performance* (Cambridge University Press 1990) 54.
[19] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147.
[20] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013) 96–102.
[21] *Mahender Chawla v Union of India* (2019) 14 SCC 615.
[22] Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006).

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

The emerging literature on AI regulation, meanwhile, warns that automated systems can reproduce discriminatory patterns if trained on biased data, and that explainability and contestability are essential where decisions affect rights and liberties.[23] Applied to witness protection, this literature suggests that AI cannot be used as a black box for categorizing witnesses or deciding eligibility for protection. Transparent standards and human oversight are indispensable.[24]

A useful way to synthesize these strands is to treat witness protection as a "high-stakes governance domain." In such domains, AI should be deployed only for bounded functions: supporting assessment, improving coordination, detecting anomalies, and documenting compliance. It should not replace legal judgment, prosecutorial discretion, or judicial supervision. This distinction is essential because witness protection often involves decisions that are ethically sensitive and procedurally consequential.

The literature also points to the role of digital identity, secure communication channels, and interoperable public infrastructure in building resilient protection systems.[25] In India, these capabilities are increasingly plausible because of ongoing digitization across administrative domains. Yet the availability of infrastructure does not itself solve legal problems. Questions of authority, standard-setting, data access, retention, liability, and review remain central. Therefore, the literature supports a balanced position: AI can make witness protection more effective, but only under a legal architecture designed for rights, oversight, and accountability.

5. Artificial Intelligence in Witness Protection: Potential Use Cases

5.1 Risk Scoring and Threat Assessment

AI could assist witness protection authorities in assessing threat levels through structured risk scoring. Such systems might combine factors such as the seriousness of the offence, prior intimidation incidents, local power dynamics, and case history to identify witnesses requiring urgent protection.[26] This may help reduce arbitrariness and improve prioritization. However, risk scoring must remain advisory, not determinative. Automated classifications can never fully capture the contextual realities of intimidation, especially in settings marked by informal coercion.

5.2 Early Warning and Anomaly Detection

Machine learning tools may detect unusual patterns, such as repeated contact attempts, digital intrusion signals, or administrative anomalies that suggest a breach in confidentiality. These systems can function as early warning mechanisms.[27] They are especially relevant where witness data is distributed across agencies and where real-time monitoring can prevent harm. Yet such monitoring raises privacy and surveillance concerns and therefore must be narrowly tailored and legally authorized.

5.3 Secure Information Management

AI-enabled platforms may help classify, encrypt, and route sensitive records according to confidentiality levels. This is especially useful in witness protection because data leakage can have immediate and severe consequences. Intelligent document management systems may also reduce human error, improve access control, and create auditable logs. In a data-intensive environment, secure information management is as important as physical protection.[28]

[23] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.
[24] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 18–24.
[25] World Bank, *World Development Report 2021: Data for Better Lives* (World Bank 2021).
[26] Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (New York University Press 2017) 79–84.
[27] OECD, *Recommendation of the Council on Artificial Intelligence* (2019) OECD/LEGAL/0449.
[28] Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008) 145–149.

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

5.4 Inter-Agency Coordination

Witness protection depends on coordination among multiple actors: police, prosecutors, trial courts, district administrations, and specialized protection units. AI-supported workflow systems can facilitate task assignment, deadline tracking, relocation coordination, and communication control. This is a classic governance problem where analytics can reduce fragmentation. Better coordination can also reduce delays, which are themselves a form of vulnerability.

5.5 Relocation and Resource Optimization

In some circumstances, witness protection involves relocation, financial assistance, transport logistics, or alternative accommodation. Decision-support tools can help allocate these scarce resources more rationally. Business analytics methods—such as queue management, resource optimization, and service routing—may be adapted to the public-sector context.[29] However, such optimization should never be purely cost-driven; the gravity of risk to life and testimony must remain the primary criterion.

5.6 Courtroom Accessibility and Testimony Support

AI-based tools may assist in secure remote testimony arrangements, witness scheduling, and communication with court administrators. They may also help reduce unnecessary exposure by enabling safer procedural pathways. Yet courtroom use must respect the accused's right to challenge evidence and the witness's right to dignity and safety. Technology should support, not displace, judicial discretion.[30]

6. Legal and Regulatory Challenges in India

6.1 Constitutional and Procedural Fairness

Any smart witness protection framework must conform to constitutional principles of fairness, equality, and liberty. Protective measures are justified when they enable participation in criminal justice without fear, but they must be carefully designed so that they do not compromise due process or create hidden procedural asymmetries. For instance, if AI systems generate risk scores that influence protection decisions, affected persons should have mechanisms to seek review, at least to the extent compatible with confidentiality. Absence of contestability would be inconsistent with principled legal governance.[31]

6.2 Privacy and Data Protection

Witness protection involves especially sensitive personal data. This includes identity, location, family details, threat information, and sometimes biometric or digital traces. AI systems thrive on data, but data concentration increases privacy risks. Any legal framework must therefore address collection limitation, purpose limitation, storage security, role-based access, retention schedules, and deletion protocols. The central regulatory question is how to enable necessary processing without normalizing over-collection.[32] This becomes even more significant when multiple agencies share databases. Strong privacy safeguards are indispensable.

6.3 Algorithmic Bias and Exclusion

AI systems are only as reliable as the data and assumptions that shape them. If historical enforcement patterns reflect underreporting, social prejudice, or uneven policing, then a risk model trained on such data may misclassify witnesses or fail to identify vulnerable populations.[33] In a socially stratified context, bias may be especially harmful. A witness from a marginalized group might either be overlooked or over-surveilled. Therefore, any AI deployment in witness protection must be subject to bias testing, calibration, and periodic review.

6.4 Transparency and Explainability

Witness protection decisions can profoundly affect personal safety and trial strategy. If AI contributes

[29] Thomas H Davenport and Jeanne G Harris, *Competing on Analytics* (Harvard Business Review Press 2017) 56–63.
[30] *State of Maharashtra v Dr Praful B Desai* (2003) 4 SCC 601.
[31] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
[32] *KS Puttaswamy v Union of India* (2017) 10 SCC 1; Digital Personal Data Protection Act 2023.
[33] Virginia Eubanks, *Automating Inequality* (St Martin's Press 2018) 127–132.

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

to those decisions, the system must be explainable to the extent necessary for administrative and judicial accountability. A fully opaque system would undermine trust and make errors difficult to detect. At the same time, some confidentiality may be necessary to protect operational security. The regulatory challenge is to reconcile transparency with protection.[34] This suggests tiered disclosure: internal auditability, judicial access, and limited external disclosure where appropriate.

6.5 Cybersecurity and Operational Integrity

The more digitized witness protection becomes, the more vulnerable it may be to cyber intrusion, insider misuse, and accidental leakage. Security is therefore a core legal issue, not a technical afterthought. Encryption, access controls, logging, incident response protocols, and vendor accountability must be addressed ex ante. A breach in witness protection data may do irreversible harm.[35] Regulatory design must therefore treat cybersecurity as an element of legal compliance.

6.6 Institutional Fragmentation and Capacity Constraints

India's criminal justice institutions often operate with uneven digital capacity. Even the best-designed AI tools can fail if staff are not trained, systems are not interoperable, or budgets are insufficient. Thus, legal reform must be accompanied by administrative modernization. Data-driven governance depends on standardized workflows, stable funding, and clear lines of authority. Without these, AI may become a layer of complexity rather than a solution.

7. Regulatory Design Principles for India

A legally viable framework for smart witness protection in India should be guided by the following principles:

7.1 Legality and Purpose Limitation

Any use of AI must be anchored in explicit legal authority and limited to defined protective purposes. Data gathered for witness protection should not be repurposed for unrelated surveillance or administrative profiling.[36]

7.2 Necessity and Proportionality

Protective interventions should be proportionate to demonstrated risk. AI should assist in calibrating the intensity of measures, not justify blanket intrusion.

7.3 Human Oversight

Final decisions affecting protection, disclosure, relocation, or confidentiality should remain subject to human judgment. AI should be advisory and auditable.[37]

7.4 Confidentiality by Design

The architecture of the system should minimize exposure by design through encryption, segmentation, need-to-know access, and secure audit trails.

7.5 Contestability and Review

Where feasible, there should be review mechanisms for decisions denying protection, modifying protection, or relying on contested risk assessments. The design of these mechanisms must preserve witness safety.

7.6 Accountability and Audit

Authorities should maintain logs, monitor performance, and evaluate whether the system reduces breaches and improves outcomes. External audit or supervisory review may be necessary to prevent abuse.[38]

[34] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76.
[35] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton 2015) 201–210.
[36] OECD, *Recommendation of the Council on Artificial Intelligence* (2019) OECD/LEGAL/0449.
[37] European Commission, *Ethics Guidelines for Trustworthy AI* (2019).
[38] NITI Aayog, *Responsible AI for All: Operationalizing Principles for Responsible AI* (Government of India 2021).

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

7.7 Equity and Non-Discrimination

The framework should be tested for disparate impact and ensure that protection is not contingent on social status, political influence, or litigation capacity.

8. Implications for Criminal Justice Efficiency

Witness protection is often discussed as a rights issue, but it is equally an efficiency issue. When witnesses are intimidated or unavailable, trials are delayed, adjournments increase, evidentiary quality deteriorates, and outcomes become less reliable.[39] These inefficiencies impose costs on courts, prosecutors, police, and litigants. In economic terms, ineffective witness protection increases transaction costs in the criminal justice system and weakens deterrence.[40] Thus, a well-designed protection regime can yield systemic gains in timeliness, credibility, and resource use.

AI and analytics can support these efficiency gains by enabling better prioritization, reducing duplication, and improving coordination.[41] However, efficiency must not be construed narrowly as speed alone. In criminal justice, efficient administration is valuable only if it is also fair, secure, and legitimate.[42] A system that moves quickly but exposes witnesses to harm or distorts procedural rights is not truly efficient in a constitutional sense.

From a governance perspective, the integration of AI into witness protection may also improve institutional learning. Aggregated data on threats, intervention success, and breach patterns can inform policy refinement. Over time, this can support evidence-based reform.[43] Yet the quality of analytics depends on the quality of data governance. Poorly structured or incomplete records will produce misleading insights.[44] Thus, analytics and law must evolve together.

9. Policy and Legal Reform Agenda

A reform agenda for India should consider the following measures:

1. **Statutory articulation of witness protection as a justiciable legal entitlement** - Protection should not depend solely on discretionary administrative practice. Its contours, eligibility criteria, and review processes should be legally structured.[45] A statutory framework would help convert witness protection from an ad hoc administrative response into a recognizable legal entitlement, thereby improving predictability and legitimacy. Such a framework should also define the minimum content of protection, the circumstances in which enhanced measures may be triggered, and the procedural obligations of the State when risk is reported.
2. **Creation or strengthening of specialized witness protection units** - These units should be trained in digital security, threat assessment, and coordinated response.[46] Specialization matters because witness protection is operationally distinct from ordinary policing. Units should have clear mandates, protected communication channels, and personnel capable of managing both physical and digital risks. Their role should extend beyond reactive escort duties to include proactive planning, case monitoring, and coordination with courts and prosecutors.

[39] Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006) 14–18.
[40] Douglass C North, *Institutions, Institutional Change and Economic Performance* (Cambridge University Press 1990) 27–35.
[41] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147, 1158–1162.
[42] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
[43] OECD, *Artificial Intelligence in Society* (OECD Publishing 2019) 95–101.
[44] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013) 50–58.
[45] *Mahender Chawla v Union of India* (2019) 14 SCC 615.
[46] Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006).

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

3. **Deployment of secure digital infrastructure** - A protected, interoperable platform should manage sensitive records, alerts, permissions, and workflow coordination. Such infrastructure should be designed to reduce fragmentation across agencies and to ensure that only authorized personnel can access relevant information. Secure infrastructure is especially important in a system where witness data may travel across multiple institutional nodes.[47] Interoperability should therefore be paired with compartmentalization so that information can be shared for legitimate protection purposes without becoming widely exposed.

4. **AI governance safeguards** - Any algorithmic component should be subjected to pre-deployment testing, bias assessment, documentation, and periodic audit. In practical terms, this means that AI tools should not be adopted simply because they are technically available or administratively attractive.[48] They must be evaluated for accuracy, fairness, reliability, and interpretability in the witness protection context. Documentation should explain the model's purpose, inputs, limitations, and governance arrangements so that legal oversight is feasible.

5. **Data protection and cybersecurity protocols** - Explicit rules should govern storage, access, transfer, retention, and deletion of witness data. The legal framework should recognize that witness protection data is exceptionally sensitive and should impose heightened security obligations accordingly. Cybersecurity measures should include encryption, access logging, incident response plans, and vendor controls.[49] These protocols should be mandatory rather than discretionary because the consequences of breach are too serious to be left to informal practice.

6. **Judicial oversight and procedural review** - Courts should retain supervisory authority over key protective measures to ensure legality and fairness. Judicial oversight is especially important where protection decisions affect anonymity, testimony arrangements, or procedural disclosure.[50] Courts need not manage operational details, but they should be able to review whether the system has acted within lawful bounds and whether proposed measures are proportionate to the risk.

7. **Capacity building** - Prosecutors, police officers, court staff, and administrative personnel should receive training in the operation and limitations of AI-supported witness protection. Capacity building is essential because technology alone cannot improve outcomes without human competence. Training should cover not only software use but also confidentiality norms, ethical constraints, escalation protocols, and the limits of algorithmic recommendations.

8. **Grievance redressal and emergency escalation pathways** - Witnesses must have safe, accessible channels to report breaches, fear, or non-compliance. These pathways should be designed to protect complainants from retaliation and to ensure rapid escalation where danger is imminent. A grievance mechanism is not merely a procedural convenience; it is a safety feature that allows the protection system to respond to changing circumstances.

9. **Periodic policy evaluation** - The system should be evaluated not only by input metrics but also by outcomes such as witness attendance, trial continuity, and breach reduction.[51] Evaluation should examine whether the system actually improves the experience of witnesses and the reliability of

[47] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[48] NITI Aayog, *Responsible AI for All: Approach Document for India* (2021).
[49] Digital Personal Data Protection Act 2023.
[50] *Zahira Habibullah Sheikh v State of Gujarat* (2004) 4 SCC 158.
[51] United Nations Office on Drugs and Crime, *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (UNODC 2008).

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 550-561 | ISSN:1505-4683

trials rather than merely increasing the number of digitally recorded actions. Outcome-based evaluation is essential because a technologically advanced system may still fail if it does not materially reduce intimidation or improve courtroom participation. The evaluation process should also inform iterative reform so that policies can be updated in light of operational experience.

This reform agenda recognizes that legal modernization is not merely about digitization. It is about constructing a credible institutional environment in which technology supports, rather than displaces, legal justice.

10. Conclusion

Witness protection occupies a foundational place in the architecture of criminal justice because the administration of truthful evidence depends on the ability of witnesses to participate without fear.[52] In India, this need is particularly acute, given the combined pressures of intimidation, institutional fragmentation, uneven administrative capacity, and the social vulnerabilities that often shape criminal litigation.[53] The analysis in this paper has shown that artificial intelligence and data-driven governance can play a meaningful supporting role in addressing these challenges by improving risk assessment, strengthening inter-agency coordination, enabling secure information management, and supporting more rational allocation of limited protective resources. Properly designed, such systems may enhance both the effectiveness and the credibility of witness protection.

At the same time, the paper has emphasized that technology cannot be treated as a substitute for legal design. Witness protection is a high-stakes domain in which errors, opacity, or data misuse may produce serious and sometimes irreversible harm. AI systems may assist in decision-making, but they also introduce risks of bias, surveillance, privacy intrusion, cybersecurity failure, and procedural unfairness.[54] For this reason, the central policy challenge is not whether India should use AI in witness protection, but under what legal conditions, with what safeguards, and under whose oversight such use should occur. The answer, as argued throughout the paper, lies in a rights-based and institutionally auditable framework grounded in legality, proportionality, human oversight, confidentiality, contestability, and accountability.

The practical implications are clear. If India seeks to render complete justice in criminal trials, witness protection must be moved from an ad hoc and reactive administrative practice toward a structured legal entitlement supported by secure digital infrastructure and clear governance protocols.[55] Specialized witness protection units, interoperable case systems, robust privacy and cybersecurity standards, and judicially reviewable decision-making can together create a more reliable protection regime.[56] Equally important, the use of analytics and AI must be accompanied by capacity building, regular audit, and outcome-based evaluation so that technological adoption does not outpace institutional readiness.[57]

Looking forward, the reform agenda should be iterative rather than static. As India's digital governance ecosystem evolves, witness protection policy should be periodically reassessed to ensure that technological tools continue to serve constitutional values and criminal justice objectives. Further research may build on this conceptual framework by examining comparative models, institutional design choices, implementation

[52] Bentham Jeremy, *Rationale of Judicial Evidence* (Hunt and Clarke 1827) vol 1, 525.

[53] *Mahender Chawla v Union of India* (2019) 14 SCC 615; Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006).

[54] European Commission, *Ethics Guidelines for Trustworthy AI* (2019); Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

[55] United Nations Office on Drugs and Crime, *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (UNODC 2008).

[56] Witness Protection Scheme 2018; *Mahender Chawla v Union of India* (2019) 14 SCC 615.

[57] Digital Personal Data Protection Act 2023; Ronald V Clarke and John Eck, *Crime Analysis for Problem Solvers in 60 Small Steps* (US Department of Justice 2005).

bottlenecks, and empirically measurable outcomes in Indian settings. Such work would strengthen the evidentiary basis for reform while preserving the paper's central normative insight: smart witness protection is valuable only when it deepens justice, protects dignity, and reinforces trust in the rule of law. Furthermore, AI can be an enabling instrument for witness protection in India, but the legitimacy of its use depends on legal discipline, regulatory restraint, and administrative accountability. The future of witness protection should therefore be neither wholly manual nor uncritically automated. It should be intelligently governed, constitutionally bound, and purposefully oriented toward the delivery of complete justice in criminal trials.

References

1. Ratanlal and Dhirajlal, *The Code of Criminal Procedure* (23rd edn, LexisNexis 2020) 12.
2. Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006) para 1.3.
3. *Zahira Habibullah Sheikh v State of Gujarat* (2004) 4 SCC 158.
4. Ranbir Singh, 'Witness Protection in India: Problems and Prospects' (2015) 57(3) Journal of the Indian Law Institute 421.
5. Ministry of Electronics and Information Technology, *National Strategy for Artificial Intelligence* (NITI Aayog 2018) 8–12.
6. Christopher Hood and Helen Margetts, *The Tools of Government in the Digital Age* (Palgrave Macmillan 2007) 67.
7. *Justice K S Puttaswamy v Union of India* (2017) 10 SCC 1.
8. Frank Pasquale, *The Black Box Society* (Harvard University Press 2015) 18–20.
9. Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006) paras 2.1–2.6.
10. Witness Protection Scheme 2018, approved in *Mahender Chawla v Union of India* (2019) 14 SCC 615.
11. Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 95–97.
12. Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 Georgetown Law Journal 1147.
13. Constitution of India, arts 14 and 21.
14. *State of Punjab v Gurmit Singh* (1996) 2 SCC 384.
15. Digital Personal Data Protection Act 2023.
16. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013) 96.
17. Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (New York University Press 2017) 42–45.
18. Douglass C North, *Institutions, Institutional Change and Economic Performance* (Cambridge University Press 1990) 54.
19. Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147.
20. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013) 96–102.
21. *Mahender Chawla v Union of India* (2019) 14 SCC 615.
22. Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006).
23. Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.
24. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 18–24.
25. World Bank, *World Development Report 2021: Data for Better Lives* (World Bank 2021).
26. Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (New York University Press 2017) 79–84.
27. OECD, *Recommendation of the Council on Artificial Intelligence* (2019) OECD/LEGAL/0449.
28. Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008) 145–149.
29. Thomas H Davenport and Jeanne G Harris, *Competing on Analytics* (Harvard Business Review Press 2017) 56–63.
30. *State of Maharashtra v Dr Praful B Desai* (2003) 4 SCC 601.
31. *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
32. *KS Puttaswamy v Union of India* (2017) 10 SCC 1; Digital Personal Data Protection Act 2023.
33. Virginia Eubanks, *Automating Inequality* (St Martin's Press 2018) 127–132.
34. Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in

the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76.
35. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton 2015) 201–210.
36. OECD, *Recommendation of the Council on Artificial Intelligence* (2019) OECD/LEGAL/0449.
37. European Commission, *Ethics Guidelines for Trustworthy AI* (2019).
38. NITI Aayog, *Responsible AI for All: Operationalizing Principles for Responsible AI* (Government of India 2021).
39. Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006) 14–18.
40. Douglass C North, *Institutions, Institutional Change and Economic Performance* (Cambridge University Press 1990) 27–35.
41. Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147, 1158–1162.
42. *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
43. OECD, *Artificial Intelligence in Society* (OECD Publishing 2019) 95–101.
44. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013) 50–58.
45. *Mahender Chawla v Union of India* (2019) 14 SCC 615.
46. Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006).
47. Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
48. NITI Aayog, *Responsible AI for All: Approach Document for India* (2021).
49. Digital Personal Data Protection Act 2023.
50. *Zahira Habibullah Sheikh v State of Gujarat* (2004) 4 SCC 158.
51. United Nations Office on Drugs and Crime, *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (UNODC 2008).
52. *Best Bakery Case: Zahira Habibullah Sheikh v State of Gujarat* (2004) 4 SCC 158.
53. Richard Susskind, *Online Courts and the Future of Justice* (Oxford University Press 2019) 82–91.
54. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 3–15.
55. European Commission, *Ethics Guidelines for Trustworthy AI* (2019).
56. Bentham Jeremy, *Rationale of Judicial Evidence* (Hunt and Clarke 1827) vol 1, 525.
57. *Mahender Chawla v Union of India* (2019) 14 SCC 615; Law Commission of India, *198th Report on Witness Identity Protection and Witness Protection Programmes* (2006).
58. European Commission, *Ethics Guidelines for Trustworthy AI* (2019); Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).
59. United Nations Office on Drugs and Crime, *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (UNODC 2008).
60. Witness Protection Scheme 2018; *Mahender Chawla v Union of India* (2019) 14 SCC 615.
61. Digital Personal Data Protection Act 2023; Ronald V Clarke and John Eck, *Crime Analysis for Problem Solvers in 60 Small Steps* (US Department of Justice 2005).