RETHINKING CYBERSECURITY IN INDIA: LEGAL CHALLENGES AND PROSPECTS OF AI-POWERED ZERO TRUST

PRASHANT KUMAR CHAUHAN

Abstract

This article reimagines India's cybersecurity paradigm in the context of the introduction of Artificial Intelligence (AI) and Zero Trust Architecture (ZTA), which significantly unites the two techniques. It discusses how AI-based ZTA can change the face of threat detection, authentication, and digital protection and reveal serious issues related to transparency, accountability, and privacy. This paper evaluates the suitability of the current legal systems in India, such as Information Technology Act, 2000 and Minimal law of Personal Data Cybersecurity: Digital Personal Information, 2023, in the effort to regulate AI-backed cybersecurity systems.

It analyses adherence to principles of equality, due process and proportionality in accordance with Articles 14 and 21 of the Indian Constitution through constitutional interpretation and juristrical enlightenment. The article features the importance of a dedicated AI-focused legal framework, ethical code of governance and institutional capacity building to consider lawful and rights-conforming cybersecurity innovation. The paper submits to conclude that AI-enabled Zero Trust has to develop into a constitutionally coherent, humane, and technologically resilient model to the digital future in India.

Keywords: *Cybersecurity, Zero Trust Architecture (ZTA), Artificial Intelligence (AI), Digital Governance, Legal Accountability.*

I. Introduction:

With the increasingly speedy process of digital transformation in the 21st century, the digital realm has not only redefined the economies, the way government takes place, as well as, personal relationships, but has also increased the threats posed by the cyber world. As there has been a transfer of sensitive governmental, financial and personal information to the cloud, on cloud-based systems, the size, complexity and sophistication of cyber threats have increased. India, similar to numerous other digitalizing countries, is on the point of the innovation and susceptibility.

Cybersecurity attack, including ransomware, outlaw access to vital databases, etc., have developed into a major threat to the national security as well as personal privacy rights.[1]

Conventional paradigms of cybersecurity, fueled by the fact that the traditional model operates based on a perimeter approach and considers the internal network as completely trusted and the external as complete distrust, have failed in this hyper scope environment. Such models do not consider the facts of remote access, real-time endpoints and increasing the Internet of Things (IoT) device breakages and thus makes digital systems more vulnerable to intrusion. To this end, it has given way to a new concept of Zero Trust Architecture (ZTA) as a paradigm of change. Based on a single rule that states the maxim of never trust and always verify, ZTA reinvents cybersecurity by removing implicit trust and implementation of authentication, authorization, and continuous monitoring around all users and systems in the system irrespective of their location or the access privileges granted to them.[2]

At the same time, the integration of Artificial Intelligence (AI) into cybersecurity ecosystems has transformed the borderlines of digital defence. Artificial intelligence-enabled tools can analyse his huge volumes in real time, identify abnormal behavioural patterns, and carry out automation to possible intrusions. This concept works together with the principle of Zero Trust in terms of improving adaptive security through the use of AI to predict threat detection and minimizing human error. Nevertheless, this convergence does come with critical legal and constitutional challenges especially in terms of privacy, due process, transparency, and algorithmic-based decision raising.

The legal framework that may be used as the foundation in the Indian context is the Information Technology Act, 2000, and the newly enacted Digital Personal Data Protection Act, 2023.[3] They however, do not sufficiently cover the issue of regulatory implications on autonomous AI systems in security architecture. As India grows into a digital-first economy with the initiatives that include

[1] *Why Cybersecurity Is Crucial for Government: Protecting Our Nation in the Digital Age*, Cybersecurity Centre of Excellence (CCoE), https://ccoe.dsci.in/blog/why-cybersecurity-is-crucial-for-government-protecting-our-nation-in-the-digital-ag (Last visited on Oct.01, 2025)

[2] Scott Rose et al., *Zero Trust Architecture*, NIST Special Publication 800-207 (Aug. 2020), https://doi.org/10.6028/NIST.SP.800-207. (Last visited on Oct.01, 2025)

[3] Hardik Beniwal, Pooja Khanna & Rajeev Kaur, *AI-Powered Personalization vs. Consumer Privacy: Striking the Balance in Indian Digital Marketing*, 2 Advances in Consumer Research 407 (2025), available at https://acr-journal.com/(Last visited on Oct.01, 2025)

Digital India and *National Cybersecurity Strategy*, there is an urgent need to understand the legal role in the regulation of AI-based Zero Trust systems.

This article aims to **critically examine how AI-powered Zero Trust models are transforming operations in cybersecurity in India. It investigates the regulatory and legal issues of models of this kind, evaluates their correspondence to the constitutional protections and questions whether the existing laws would be too insufficient to raise security frustrations and the civil liberties concerns. The discussion also uses international they have set and their best practices to provide a rights-based, responsible, and proactive roadmap on cybersecurity governance in India.**

II. Conceptual Framework (Zero Trust and AI Integration):

The modern cybersecurity paradigm is shifting away from the traditional perimeter-centric models toward architectures that prioritize verification and adaptive security at every level. Zero Trust Architecture (ZTA) is one such transformative approach, premised on the idea that no user, device, or network component should be inherently trusted regardless of whether it is inside or outside the organization's security perimeter. Instead, ZTA mandates continuous verification, context-aware access control, and behavior-based monitoring as foundational principles of secure system design.[4]

A. Principles of Zero Trust Architecture:

ZTA operates on several key principles that redefine the security posture of digital infrastructures:

- **Continuous Verification:** Every access request must be authenticated and authorized in real time, based on contextual information such as user identity, device health, and geolocation.[5]
- **Least Privilege Access:** Users are granted only the minimum level of access required to perform their tasks, thereby reducing the attack surface.[6]

[4] John Kindervag, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, Forrester Research (2010).

[5] National Institute of Standards and Technology, *Special Publication 800-207: Zero Trust Architecture*, (2020), available at https://nvlpubs.nist.gov (last visited Sept.15, 2025).

[6] Ibid.

- **Micro-Segmentation:** Networks are compartmentalized into isolated segments to limit lateral movement by adversaries, ensuring that a breach in one segment does not compromise the entire system.[7]
- **Assume Breach Mentality:** The architecture is designed with the assumption that attackers may already be present in the network, thus emphasizing containment, logging, and incident response.[8]

B. Role of Artificial Intelligence in Enhancing ZTA:

The introduction of Artificial Intelligence (AI) into Zero Trust systems substantially augments their efficacy. AI algorithms, particularly those rooted in machine learning (ML), can analyze vast amounts of user data and system logs to detect deviations from normal behavior.[9] Through anomaly detection, user behavior analytics (UBA), and threat intelligence correlation, AI enhances the dynamic adaptability of ZTA by making real-time decisions about access permissions and potential intrusions.

This AI-enabled capability is not static; it learns and evolves based on feedback loops and ongoing data analysis. As a result, security systems become proactive rather than reactive, capable of predicting threats before they materialize and automating responses to minimize human delay and error.[10]

However, the use of AI in such security-critical contexts raises essential legal concerns regarding opacity, autonomy, and accountability. AI decisions that restrict access, deny service, or trigger surveillance must adhere to constitutional and statutory mandates of fairness, transparency, and non-arbitrariness, especially under Articles 14 and 21 of the Indian Constitution.[11]

C. Legal Doctrines Supporting Zero Trust Integration:

The shift toward AI-powered ZTA must be interpreted in light of well-established legal doctrines:

[7] Microsoft, *Zero Trust Deployment Guide*, (2021), available at https://docs.microsoft.com (last visited Sept.15, 2025).

[8] Ibid.

[9] NidhiRastogi and James Hendler, "A Survey of AI Methods for Cybersecurity Intrusion Detection," (2020) 3 *ACM Computing Surveys* 1.

[10] R. Bace and P. Mell, *Intrusion Detection Systems*, NIST Special Publication 800-31 (2001).

[11] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

- **Precautionary Principle:** Originally evolved in environmental law, this principle justifies pre-emptive actions in the face of uncertain threats. Applied to cybersecurity, it supports the design of systems that assume breach and respond with maximal caution.[12]
- **Doctrine of Proportionality:** Any measure that affects individual rights such as AI-enabled surveillance or access denial must be legally sanctioned, necessary for a legitimate aim, and proportionate to that aim.[13]
- **Due Process and Reasoned Decision-Making:** The Indian legal system mandates that actions affecting individual rights must be backed by intelligible reasons and offer avenues for redress. AI systems must, therefore, incorporate explainability and grievance mechanisms to comply with procedural fairness.[14]

Thus, while AI-ZTA integration offers technological sophistication, it demands a regulatory framework that harmonizes cyber-resilience with legal defensibility. This requires a multidisciplinary approach, blending insights from computer science, law, ethics, and public policy. The next section will assess how global and Indian legal frameworks are responding to this convergence.

III. Legal and Regulatory Framework in India:

The deployment of AI-powered Zero Trust Architecture (ZTA) raises significant regulatory and constitutional implications in India. With the spread of the digital infrastructure landscape, the legal system of India is increasingly being challenged to embrace the perception of the complexity of algorithmic decision making, surveillance in general and evolving systems based on access control. Even though there are a number of laws, policy statements and court rulings that talk about cybersecurity and data protection, it is still difficult to have a unified regulatory structure geared specifically towards the issues of AI-enhanced ZTA.

[12] ShibaniGhosh, "Application of the Precautionary Principle in Indian Environmental Cases," (2013) 5 *Journal of Environmental Law* 1.

[13] *Modern Dental College and Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.

[14] *Union of India v. Tulsiram Patel*, AIR 1985 SC 1416.

A. Information Technology Act, 2000 and Allied Rules:

In India, the key legislation that acts as the basis of laws on cybersecurity and digital governance is still Information Technology Act, 2000 (IT Act). Introduced in the name of allowing an electronic transaction recognition in the law, it has had numerous changes to accommodate the emerging issues, to deal with cybercrime. [15]

Section 43A seeks to hold corporate organizations liable when they have failed to safeguard sensitive personal data by employing reasonable security measures. [16] In the same way, Section 72A punishes the unlawful transfer of information by service providers.[17] Though these provisions are quite broad-based, AI-driven autonomous systems are not explicitly addressed, nor it is specified that the explainability of decision-making gaps should be enforced, and it becomes especially critical when AI assumes control to either deny access or engage in surveillance, which occurs in Zero Trust contexts.

In addition, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 require the minimum standards of protecting the data but do not refer to the topic of the algorithmic decision-making and automatic response to threats or governance of AI.[18]

B. Digital Personal Data Protection Act, 2023:

The recently enacted Digital Personal Data Protection Act, 2023 has brought a significant improvement in the sphere of data protection in India. It introduces concepts of data minimization, purpose limitation, and data fiduciary accountability and establishes the foundations of stronger digital privacy rights. [19]

[15] Information Technology Act, 2000, No. 21 of 2000, India Code (2000).

[16] Ibid, s. 43A.

[17] Ibid, s. 72A.

[18] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E).

[19] Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

Section 8 places the duty on all the data fiduciaries to provide justifiable security measures to avert personal data breaches. [20]

However, the Act does not address the explainability, auditability, or transparency of AI-based systems involved in these safeguards. The absence of specific obligations for automated decision-making, profiling, or the right to object to algorithmic outcomes limits its applicability in the context of AI-ZTA integration.

Furthermore, the Data Protection Board of India, established under the Act, has not yet issued any binding regulatory guidelines on AI use in cybersecurity, leaving a substantial legal vacuum.[21]

C. CERT-In Guidelines (April 2022):

The Indian Computer Emergency Response Team (CERT-In), operating under the Ministry of Electronics and Information Technology (MeitY), issued revised cybersecurity guidelines in April 2022. These mandate mandatory breach reporting within six hours and require organizations to maintain logs for 180 days.[22] These measures significantly enhance India's incident response framework.

Nevertheless, the guidelines lack any reference to AI-specific implementation or accountability standards for autonomous systems. As a result, while they strengthen procedural compliance, they do not account for the unique operational dynamics and risks of AI-powered Zero Trust systems, such as false positives, automated lockdowns, and discriminatory access decisions.

D. Judicial Pronouncements and Constitutional Safeguards:

Indian constitutional jurisprudence has progressively evolved to address digital privacy and data governance concerns. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court affirmed that the right to privacy is a fundamental right under Article 21 of the Constitution.[23] The Court emphasized the principles of legality, necessity, and proportionality for any state action infringing upon privacy.[24] These principles are particularly relevant for ZTA models, where

[20] Ibid, s. 8.

[21] Ibid, ss. 19-21.

[22] Indian Computer Emergency Response Team, Guidelines for Information Security Practices (April 28, 2022), available at https://www.cert-in.org.in (last visited Sept.18, 2025).

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

[24] Ibid.

continuous authentication and real-time surveillance could potentially infringe on informational autonomy.

Moreover, the decision in *Maneka Gandhi v. Union of India* established that any executive action affecting personal liberty must adhere to procedural due process.[25] This has direct implications for AI systems that autonomously determine access to digital platforms, services, or institutional networks.

Judicial interpretations also provide safeguards under Article 14, prohibiting arbitrary or discriminatory decision-making. Algorithmic opacity or biased training data within ZTA systems may thus attract constitutional scrutiny.

E. Gaps and the Need for Legal Reform:

Despite the emergence of sectoral guidelines from regulators like the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority of India (IRDAI), and Securities and Exchange Board of India (SEBI)each mandating cybersecurity best practices there exists no unified framework addressing AI-ZTA. These regulatory instruments, while encouraging enhanced cyber hygiene, fail to govern algorithmic governance, transparency standards, or liability in cases of AI malfunctions.[26]

The absence of a comprehensive AI legislation, and the delay in implementing the National Cybersecurity Strategy, further deepens regulatory fragmentation. As AI-powered ZTA models become integral to both public and private sector digital infrastructures, the Indian legal system must urgently re-evaluate its current statutes to ensure constitutional and procedural compatibility.

IV. Constitutional and Ethical Dimensions:

The integration of Artificial Intelligence into Zero Trust Architecture (ZTA) represents a powerful innovation in cybersecurity. However, it also raises complex constitutional, ethical, and jurisprudential issues, especially in the Indian context where fundamental rights and state accountability are deeply enshrined in the legal framework. The shift from human-centered decision-making to algorithmically governed access controls and behavioral monitoring invites a

[25] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.

[26] Reserve Bank of India, *Cybersecurity Framework in Banks* (2016); IRDAI Guidelines on Information and Cyber Security (2017); SEBI Cybersecurity and Cyber Resilience Framework (2019).

re-evaluation of how principles like equality, privacy, and procedural fairness apply in digital systems. As AI-enabled ZTA systems are increasingly adopted by public institutions, critical sectors, and governance platforms, ensuring compliance with constitutional norms becomes imperative.

A. Right to Equality and Algorithmic Bias (Article 14): Article 14 of the Indian Constitution guarantees equality before the law and prohibits arbitrary or discriminatory treatment by state and non-state actors.[27] AI algorithms trained on historical or biased datasets may inadvertently reinforce existing inequalities.[28] For instance, an AI system deployed within a Zero Trust framework might flag or restrict access based on behavioral anomalies that correlate with socio-economic, regional, or linguistic patterns without malicious intent but with discriminatory outcomes.

The lack of transparency in how AI models evaluate risk or define anomalies may result in arbitrary classifications that do not withstand judicial scrutiny. As held in *E.P. Royappa v. State of Tamil Nadu*, arbitrariness is antithetical to equality.[29] Therefore, algorithmic decisions that affect user access or privileges must be auditable and explainable to meet the threshold of non-arbitrariness under Article 14.

B. Right to Privacy and Surveillance (Article 21): The right to privacy, now recognized as a fundamental right under Article 21, was firmly established by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[30] The Court laid down the three-fold test legality, necessity, and proportionality for any infringement of this right.

AI-powered ZTA systems continuously monitor user behavior, device activity, access requests, and network traffic. If implemented without purpose limitation, minimal data collection, or oversight mechanisms, such surveillance could lead to profiling, behavioral prediction, and potential chilling effects on freedom of expression.[31] Particularly in government systems, these

[27] Constitution of India, art. 14.

[28] Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," (2016) 104 *California Law Review* 671.

[29] *E.P. Royappa v. State of Tamil Nadu*, AIR 1974 SC 555.

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

[31] VrindaBhandari and UjwalSagar, "Chilling Effect of Surveillance in India," (2021) 13 *NUJS Law Review* 1.

models may resemble surveillance infrastructures rather than security tools unless carefully regulated.

The principle of informational autonomy, developed in *Puttaswamy*, implies that individuals have the right to control how their personal data is accessed and processed.[32] Unchecked AI surveillance violates this autonomy and risks infringing upon personal liberty and dignity, even if conducted under the guise of national security or efficiency.

C. Due Process and the Right to a Reasoned Decision: As established in *Maneka Gandhi v. Union of India*, any deprivation of life or liberty must follow a just, fair, and reasonable procedure.[33] AI-enabled systems that make autonomous decisions such as denying access, flagging security threats, or triggering account lockdowns must offer users explanation rights, review mechanisms, and redressal avenues.

The problem of "black-box AI"where decision logic is inscrutable poses a direct challenge to natural justice, which requires audi alteram partem and the provision of reasons for adverse decisions.[34] The use of explainable AI (XAI) models in ZTA is therefore not just a technological improvement but a constitutional necessity to ensure procedural fairness.

D. Ethical Considerations and the Precautionary Principle: From an ethical standpoint, the deployment of AI in sensitive environments such as law enforcement, healthcare, or finance requires proactive safeguards. The Precautionary Principle, widely recognized in Indian environmental jurisprudence, is equally applicable here.[35] If a system's functioning could lead to harm, bias, or rights violations even without full empirical certainty its use must be governed by strict ethical and legal oversight.

This principle mandates that AI-ZTA systems must be developed and deployed under a framework that anticipates misuse, enforces transparency, and requires continuous ethical evaluations.

E. Balancing State Interest and Individual Rights: While the State has a legitimate interest in securing digital infrastructure and critical systems, it cannot override fundamental rights in the

[32] *Justice K.S. Puttaswamy (Retd.) v. Union of India*.

[33] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.

[34] Sandra Wachter et al., "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] *Vellore Citizens Welfare Forum v. Union of India*, AIR 1996 SC 2715.

name of efficiency or automation. The Court in *Modern Dental College v. State of Madhya Pradesh* emphasized that any infringement of individual rights must be proportionate to the aim pursued and the least restrictive means available.[36] In the context of ZTA, this means deploying privacy-preserving AI models, allowing opt-out mechanisms where feasible, and subjecting surveillance systems to judicial or independent oversight.

V. Benefits and Use Cases of AI-Powered ZTA:

While the legal and ethical concerns surrounding AI-integrated Zero Trust Architecture (ZTA) are significant, these systems also offer powerful advantages in promoting cyber resilience, regulatory compliance, and rights-based governance. When implemented transparently and ethically, AI-ZTA systems can enhance data protection, streamline accountability mechanisms, and reduce the burden on manual cybersecurity protocols. In India, where digital governance is rapidly expanding across sectors, the integration of AI with ZTA has the potential to establish robust, adaptable, and constitutionally sound security frameworks.

A. Strengthening Legal Compliance and Cyber Hygiene: One of the most direct benefits of AI-powered ZTA is the facilitation of compliance with statutory obligations under laws such as the Digital Personal Data Protection Act, 2023 (DPDPA) and the Information Technology Act, 2000. These laws require entities to adopt reasonable security safeguards, minimize data exposure, and respond to breaches swiftly.[37]

AI-enhanced ZTA inherently supports these goals by:

- Restricting access through behavior-based policies and contextual verification;
- Maintaining real-time logs that can serve as evidence in regulatory investigations;
- Flagging anomalies proactively, often before breaches occur.

These systems also help organizations comply with CERT-In's 2022 Guidelines, which mandate the retention of logs for 180 days and reporting of security incidents within six hours.[38] By automating these processes, AI-ZTA reduces human error and ensures timely compliance.

[36] *Modern Dental College and Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.

[37] Digital Personal Data Protection Act, 2023, s. 8; Information Technology Act, 2000, s. 43A.

[38] Indian Computer Emergency Response Team (CERT-In), Guidelines for Cyber Incident Reporting, April 28, 2022, available at https://www.cert-in.org.in (last visited Sept. 19, 2025).

B. Enhancing Transparency and Institutional Accountability: AI-ZTA systems, when built with explainable AI (XAI) frameworks, enhance transparency in cybersecurity decisions. When access is denied or behavior is flagged as anomalous, a well-designed system can provide reason codes, audit trails, and decision logs thereby satisfying constitutional and administrative law requirements for reasoned decisions.[39]

Such features are particularly relevant for public institutions and regulated sectors, where decisions affecting individuals must be justifiable and reviewable. For instance, under Article 14 of the Constitution, non-arbitrariness is a fundamental requirement for administrative actions.[40] Transparent AI-ZTA systems help ensures that cyber risk responses are based on objective parameters rather than subjective discretion or opaque algorithms.

C. Sector-Specific Applications and Legal Implications: Several Indian sectors stand to benefit significantly from the deployment of AI-integrated Zero Trust models:

- **Banking and Financial Sector:** Regulated by the Reserve Bank of India (RBI), banks and financial institutions must implement risk-based authentication, real-time fraud detection, and access controls.[41] AI-ZTA supports these mandates by detecting anomalous transaction behavior, identifying insider threats, and maintaining forensic-ready logs. This aids compliance with anti-money laundering (AML) and Know Your Customer (KYC) obligations.

- **Healthcare and Health-Tech Systems:** Electronic Health Records (EHRs) are considered sensitive personal data, requiring the highest levels of protection under the DPDPA.[42] AI-ZTA can enforce strict access protocols, detect unauthorized attempts to access records, and prevent misuse thereby fulfilling both Indian and international data protection standards like HIPAA in cross-border settings.[43]

[39] Sandra Wachter, Brent Mittelstadt& Chris Russell, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR," (2018) 31 *Harvard Journal of Law & Technology* 841.

[40] *E.P. Royappa v. State of Tamil Nadu*, AIR 1974 SC 555.

[41] Reserve Bank of India, Cyber Security Framework in Banks, Circular No. RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, (Jun. 2, 2016).

[42] Digital Personal Data Protection Act, 2023, s. 3(d).

[43] Health Insurance Portability and Accountability Act (HIPAA), 1996 (U.S.).

- **E-Governance and Judiciary:** With the digitization of public services and judicial records, ZTA ensures controlled access to sensitive platforms, tamper-proof documentation, and auditability of access to citizen databases. In judicial administration, it aids in preserving chain of custody, a critical component for digital evidence admissibility.[44]

- **Critical Infrastructure and Utilities:** The Information Technology Act, 2000, under Section 70, designates certain sectors such as power, telecom, and financial systems as Critical Information Infrastructure (CII).[45] For these systems, AI-ZTA offers predictive threat detection, automated isolation of infected nodes, and national security-grade resilience.

D. Constitutional Alignment and Rights-Based Governance: AI-powered Zero Trust, if designed ethically, does not inherently conflict with constitutional mandates. On the contrary, it can:

- Safeguard privacy (Article 21) through minimized data exposure and purpose-limited access;[46]

- Prevent discrimination (Article 14) by replacing ad hoc human discretion with standardized algorithms, subject to bias checks;

- Promote accountability by ensuring that all access decisions are logged, explainable, and reviewable, satisfying procedural fairness under *Maneka Gandhi* and *Puttaswamy rulings*.[47]

Thus, the AI-ZTA model, while technologically advanced, also lends itself to strengthening legal defensibility and upholding democratic values. The caveat, however, lies in implementation fidelity without ethical design, auditability, and oversight, even the most promising systems can become instruments of overreach.

VI. Legal and Regulatory Challenges:

[44] *State v. Mohd.Afzal*, (2003) DLT 385 (Del).

[45] Information Technology Act, 2000, s. 70.

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

[47] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.

Despite the promising legal and technical potential of AI-powered Zero Trust Architecture (ZTA), its widespread deployment in India presents a complex array of legal, regulatory, and constitutional challenges. As AI systems become more autonomous and deeply embedded in decision-making processes related to access, authentication, and surveillance, they bring forth dilemmas that traditional legal frameworks are ill-equipped to resolve. The absence of clear accountability structures, transparency norms, and cross-border safeguards further complicates the regulatory landscape. These issues require immediate attention to prevent systemic violations of rights and ensure the lawful implementation of such advanced cybersecurity models.

A. Algorithmic Bias and Discriminatory Decision-Making: One of the primary concerns associated with AI in cybersecurity is the risk of algorithmic bias. AI models often rely on historical datasets for training. If these datasets reflect underlying societal prejudices whether based on geography, gender, caste, or socioeconomic status the resulting decisions may reproduce and even magnify discriminatory outcomes.[48]

Under Article 14 of the Indian Constitution, any classification must be reasonable and non-arbitrary.[49] If an AI system integrated into ZTA disproportionately flags or restricts individuals from certain demographics without clear justification, it may violate the right to equality. The absence of mandated audits or bias testing mechanisms in India's current legal regime leaves these violations unaddressed and potentially unaccountable.

B. Lack of Transparency and Explainability: Most AI systems used in cybersecurity operate as "black boxes", where the internal logic of decision-making is opaque even to their developers.[50] This creates significant barriers to legal scrutiny, especially when access to essential services or platforms is denied based on automated assessments.

The principle of natural justice, derived from *Maneka Gandhi v. Union of India*, requires that affected individuals be given reasons for adverse decisions and a fair opportunity to respond.[51] In the context of ZTA, unexplained access denials, automated lockdowns, or behavioral flags could violate the right to procedural fairness under Article 21.

[48] NITI Aayog, *Responsible AI: A Strategy for India*, Discussion Paper (2021), p. 15.

[49] *E.P. Royappa v. State of Tamil Nadu*, AIR 1974 SC 555.

[50] Brent Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," (2016) 3 *Big Data & Society* 1.

[51] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.

India lacks any statutory requirement for explainability-by-design in AI systems, rendering current frameworks insufficient to ensure transparency and redressal in AI-powered cybersecurity mechanisms.

C. Accountability and Attribution of Legal Liability: AI-powered ZTA systems challenge traditional notions of accountability. In conventional systems, decisions can be traced to a human authority. In contrast, autonomous systems make independent judgments, triggering actions such as access denial, surveillance, or risk quarantines.

The Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 impose obligations on “data fiduciaries” and “intermediaries”, but they do not delineate responsibility for AI-generated decisions.[52] If a breach occurs due to an AI system's false negative, or if legitimate users are wrongfully blocked, questions arise:

- Is the liability on the organization deploying the AI?
- Is the developer or AI vendor responsible?
- Can autonomous systems themselves be held legally liable?

The absence of a dedicated AI legislation in India means that these questions remain unresolved, posing significant risk for both organizations and individuals.

D. Privacy Infringement and Mass Surveillance Risks: ZTA relies on continuous behavioral monitoring and system telemetry to validate user authenticity. When combined with AI, this transforms into a form of predictive surveillance, which if not regulated may intrude upon personal autonomy and dignity.

The Puttaswamy judgment mandates that any state action infringing privacy must be legal, necessary, and proportionate.[53] However, most AI-ZTA systems are deployed without individualized consent, without public oversight, and often operate under internal policies that are not publicly disclosed.

In the absence of purpose limitation, data retention norms, or user opt-out rights, these systems can become mass surveillance infrastructures, violating Articles 21 and 19(1)(a) of the Constitution.

[52] Information Technology Act, 2000, ss. 43A, 72A; Digital Personal Data Protection Act, 2023, ss. 8-10.

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

E. Cross-Border and Jurisdictional Complications: A significant portion of AI-based cybersecurity infrastructure is hosted on cloud platforms and integrated with foreign vendors. This raises concerns regarding:

- Cross-border data transfers;
- Jurisdictional enforcement of liabilities;
- Compliance with Indian laws when data resides outside Indian territory.

The DPDPA, 2023 is silent on the issue of data localization or adequacy standards for international data transfer, creating uncertainty for entities relying on foreign-hosted AI-ZTA tools.[54] Moreover, in case of disputes or breaches, jurisdictional enforcement becomes complex, especially when the AI tool's design, training, or storage occurs in foreign jurisdictions.

India's failure to adopt a comprehensive cross-border data regulation regime puts organizations at risk of non-compliance, especially in sectors dealing with sensitive personal or national data.

VII. Policy Recommendations and Way Forward:

To ensure that AI-powered Zero Trust systems serve as tools of both cybersecurity and constitutional compliance, India must adopt a forward-looking regulatory strategy. This section outlines key recommendations for legal, institutional, and ethical reforms which are as following:

A. **Enact a Comprehensive AI Regulation:** India needs a dedicated legal framework to govern AI, addressing transparency, algorithmic accountability, and liability attribution. Such legislation should mandate explainability-by-design, risk classification, and impact assessments for AI systems used in security-critical sectors.

B. **Promote Cross-Border Cooperation:** India should engage with global frameworks like the OECD AI Principles and GPAI, and develop bilateral agreements to manage cross-border data transfers and ensure vendor accountability.

C. **Embed Ethical Standards in Cybersecurity Protocols:** The Ministry of Electronics and Information Technology (MeitY) and CERT-In should issue AI-specific ethical guidelines for ZTA, emphasizing privacy-preserving architectures, minimal data collection, and grievance redressal mechanisms.

[54] Digital Personal Data Protection Act, 2023, ch. VI.

D. **Build Judicial and Institutional Capacity:** Training modules on AI and cybersecurity law should be introduced in Judicial Academies, Bar Councils, and civil service training institutes to equip public authorities with the capacity to evaluate and regulate AI-powered systems.

E. **Strengthen Sectoral Oversight and Compliance:** Regulators like RBI, IRDAI, and SEBI must adopt sector-specific compliance checklists for AI-ZTA, including technical benchmarks, documentation standards, and audit mechanisms to ensure procedural fairness.

VIII. Conclusion:

AI-powered Zero Trust Architecture marks a paradigm shift in cybersecurity by enabling adaptive, predictive, and continuous protection of digital assets. In India's rapidly digitizing environment, such systems can enhance national security, data protection, and regulatory compliance. However, their deployment also presents novel challenges related to privacy, algorithmic transparency, accountability, and constitutional safeguards.

While the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 provide a foundational legal basis, they remain insufficient to address the complexities of autonomous AI systems operating in critical security roles. Constitutional principles especially those arising from *Puttaswamy* and *Maneka Gandhi* require that AI systems embedded in public and private infrastructures uphold due process, equality, and the right to privacy.

To ensure that cybersecurity advances do not come at the expense of civil liberties, India must adopt a comprehensive regulatory framework for AI, establish ethical standards in cybersecurity governance, and strengthen institutional capacity across sectors. AI-powered Zero Trust should not merely be a technological innovation it must function as a legally robust, ethically grounded, and rights-preserving standard for digital security in a democratic society.