Advances in Consumer Research
https://acr-journal.com/
ISSN: 0098-9258
ISSN: 3079-1766
Volume-3 | Issue-2 | Feb 2026

Original Researcher Article

Ai-Enabled Cybersecurity And Privacy Governance In India: Comparative Insights From The European Union

Dr. Vaishali[1], Mr. Jeevan Thombare[2]
[1] Assistant Professor, School of Law, UPES, Dehradun.
Email: vsingh3803@gmail.com
[2] Research Fellow, Ratan Tata Maharashtra State Skills University, Mumbai.
Email: jeevan.mplcon@gmail.com

ABSTRACT
The growing reliance on artificial intelligence in cybersecurity has significantly altered how digital threats are monitored, assessed, and addressed. In India, both public and private actors increasingly deploy AI-enabled cybersecurity systems capable of continuous data monitoring, automated threat detection, and real-time response. While these technologies promise enhanced security and efficiency, their operation raises serious concerns regarding privacy protection, accountability, and legal responsibility. Existing Indian legal frameworks, particularly the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000, were developed on the assumption of human-controlled decision-making and offer limited guidance on the governance of autonomous or semi-autonomous AI systems used in cybersecurity contexts. This paper critically examines whether India's current privacy and data protection regime is equipped to regulate AI-driven cybersecurity systems without undermining fundamental rights. Using a doctrinal research methodology supplemented by comparative legal analysis, the study evaluates the Indian regulatory framework alongside the European Union's General Data Protection Regulation and the EU Artificial Intelligence Act. The comparative analysis demonstrates that while the EU has adopted a risk-based approach that explicitly addresses high-risk AI systems and accountability obligations, Indian law remains largely technology-neutral and silent on questions of AI autonomy and liability. The paper argues that AI-enabled cybersecurity challenges traditional legal concepts of consent, proportionality, and fault, particularly where continuous surveillance and automated decision-making affect individuals without meaningful human intervention. It further highlights emerging governance gaps relating to liability attribution between system developers, deployers, and state authorities. The study concludes by proposing targeted regulatory and policy reforms aimed at strengthening accountability mechanisms, embedding privacy-by-design principles, and aligning India's cybersecurity governance with evolving global standards, while remaining sensitive to domestic constitutional and institutional realities..

Keywords: AI-Driven Cybersecurity, Privacy and Data Protection Law, Digital Personal Data Protection Act, 2023, AI Accountability and Liability, Cyber Surveillance and Consent, EU Artificial Intelligence Act, Comparative Technology Law.

INTRODUCTION:

The deployment of artificial intelligence (AI) in cybersecurity governance represents a structural transformation in how states and private actors conceptualise, prevent, and respond to digital threats. Unlike conventional cybersecurity tools that operate through static rules and predefined thresholds, AI-enabled systems are capable of autonomous learning, predictive threat modelling, continuous behavioural surveillance, and real-time adaptive response. These capabilities have become increasingly central to addressing sophisticated cyber threats such as zero-day exploits, advanced persistent threats, and large-scale data breaches that exceed human response capacities (ENISA, 2023; OECD, 2022).

In India, the adoption of AI-driven cybersecurity solutions has accelerated across sectors including banking and finance, telecommunications, critical infrastructure, digital public platforms, and law enforcement. This trend is closely linked to the state's broader digital governance agenda, the expansion of data-intensive public infrastructures, and the growing reliance on automated risk-management systems in both public and private domains (MeitY, 2023; NITI Aayog, 2024). However, the rapid integration of AI into cybersecurity architectures has not been matched by a corresponding evolution in legal and regulatory frameworks governing privacy, accountability, and individual rights.

AI-enabled cybersecurity systems function through continuous data monitoring, pattern recognition, and automated decision-making. In practice, this entails large-scale processing of personal data, metadata, and

behavioural information, often without the direct knowledge or meaningful consent of affected individuals. Such practices challenge foundational principles of privacy and data protection law, including purpose limitation, data minimisation, proportionality, and human accountability. Where cybersecurity decisions—such as access denial, system isolation, or user flagging—are generated autonomously, traditional legal doctrines premised on human intent, fault, and control become increasingly difficult to apply (Floridi et al., 2023; Solove, 2024).

India's existing legal framework governing data protection and cybersecurity was not designed with autonomous AI systems in mind. The Information Technology Act, 2000 conceptualises cybersecurity largely through the lens of human-controlled systems, focusing on cyber offences, due-diligence obligations, and institutional response mechanisms. More recently, the Digital Personal Data Protection Act, 2023 (DPDP Act) has sought to establish a comprehensive data protection regime grounded in consent, lawful processing, and fiduciary accountability. While the Act marks an important legislative milestone, it remains largely silent on the governance of AI-driven decision-making, particularly in cybersecurity contexts where automated systems may generate significant legal or practical effects for individuals (Bhatia, 2023; Ramanathan, 2024).

This regulatory silence becomes more pronounced when contrasted with developments in the European Union. The EU's General Data Protection Regulation (GDPR) explicitly recognises the risks associated with automated decision-making and profiling, embedding rights-based safeguards against purely automated determinations. Building on this foundation, the European Union Artificial Intelligence Act adopts a risk-based regulatory model that directly addresses high-risk AI systems, including those deployed in cybersecurity and critical infrastructure protection. Together, these instruments reflect a shift from formal technology-neutrality towards AI-sensitive governance that foregrounds accountability, human oversight, and fundamental rights protection (European Commission, 2024; Veale & Borgesius, 2023).

Against this background, this paper critically examines whether India's current privacy and data protection regime is capable of regulating AI-enabled cybersecurity systems without undermining constitutional guarantees and fundamental rights. Employing a doctrinal research methodology supplemented by comparative legal analysis, the study evaluates Indian law alongside the EU's regulatory framework to identify governance gaps, accountability deficits, and normative challenges. It argues that while India's flexible and technology-neutral approach offers adaptability, it inadequately addresses the autonomy, opacity, and rights-impacting potential of AI-driven cybersecurity systems.

The central claim advanced is that AI-enabled cybersecurity fundamentally alters the balance between security imperatives and privacy guarantees, necessitating a recalibration of legal principles governing consent, proportionality, and liability. By drawing comparative insights from the EU's risk-based approach, the paper proposes targeted reforms aimed at strengthening accountability, embedding privacy-by-design, and aligning India's cybersecurity governance with evolving global standards, while remaining attentive to domestic constitutional norms and institutional capacities.

Conceptual Foundations: AI, Cybersecurity, and Privacy Governance

AI-enabled cybersecurity systems differ qualitatively from traditional digital security tools. Rather than merely executing predefined instructions, these systems analyse vast datasets to identify patterns, predict vulnerabilities, and initiate responses with minimal or no human intervention. Machine learning algorithms, for instance, can infer behavioural norms, detect anomalies, and adapt security protocols dynamically. While this enhances efficiency and responsiveness, it simultaneously reduces transparency and human control.

From a legal perspective, the defining challenge posed by AI in cybersecurity lies in its autonomy. Autonomy complicates attribution of responsibility, as decisions emerge from probabilistic models rather than direct human command. This disrupts established legal doctrines premised on identifiable decision-makers and intentional conduct. In cybersecurity contexts, where automated actions may have immediate and significant consequences for individuals such as denial of access, account suspension, or increased surveillance—the absence of clear accountability mechanisms raises serious rule-of-law concerns.

Privacy governance traditionally operates through a combination of consent, purpose limitation, and proportionality. AI-enabled cybersecurity strains each of these principles. Consent becomes diluted where data collection is continuous and embedded within system architecture. Purpose limitation is challenged when AI systems repurpose data for evolving threat models. Proportionality becomes difficult to assess when surveillance is automated, scalable, and opaque.

In constitutional democracies, cybersecurity governance must therefore be evaluated not only in terms of effectiveness but also in relation to fundamental rights. In India, the recognition of privacy as a constitutionally protected right has imposed substantive limits on state surveillance and data processing. However, the application of these limits to AI-driven systems remains underdeveloped in statutory and judicial discourse.

This conceptual tension between security imperatives and rights-based governance forms the analytical foundation of this paper. By situating AI-enabled cybersecurity within broader debates on autonomy, accountability, and constitutionalism, the study underscores the need for regulatory frameworks that move beyond formal neutrality and engage directly with the distinctive risks posed by AI.

Literature Review

This section surveys scholarly debates on AI-driven cybersecurity, privacy, and regulation across global and Indian contexts. While EU scholarship has developed risk-based governance models, Indian literature remains largely technology-neutral. This paper addresses this gap by focusing specifically on AI-enabled cybersecurity governance.

Academic discourse on AI-enabled cybersecurity consistently emphasises that artificial intelligence has altered not merely the tools of cybersecurity, but the very *governance logic* underpinning digital security. Traditional cybersecurity models relied on static rules, human-defined thresholds, and post-incident response. By contrast, AI-driven systems operate through continuous learning, predictive analytics, and automated enforcement, enabling pre-emptive security interventions (Buchanan, 2020).

Scholars note that this shift introduces a governance paradox: while AI enhances efficiency and threat responsiveness, it simultaneously reduces transparency and human oversight. Algorithms trained on vast datasets make security decisions that are difficult to explain even to system designers, thereby undermining established legal expectations of explainability and accountability (Pasquale, 2015). In cybersecurity contexts, this opacity is particularly problematic because decisions often involve intrusive data processing and immediate restrictions on individual access or behaviour.

Legal scholarship has increasingly recognised that AI-enabled cybersecurity should not be treated as a neutral technical enhancement. Instead, it represents a form of *algorithmic governance* that redistributes power between states, private actors, and individuals. As DeNardis (2020) observes, cybersecurity infrastructures increasingly function as regulatory systems in their own right, shaping rights, obligations, and risk distribution without explicit democratic authorization.

The intersection of AI-driven cybersecurity and privacy has been extensively debated in surveillance studies and data protection literature. A central concern is the erosion of meaningful consent in environments characterised by continuous, automated data collection. Zuboff's concept of "surveillance capitalism" highlights how behavioural data is routinely extracted and analysed in ways that exceed individuals' reasonable expectations, a critique that applies with equal force to cybersecurity surveillance architectures (Zuboff, 2019).

From a legal standpoint, scholars argue that consent-based privacy frameworks are ill-suited to AI-enabled systems that operate invisibly and autonomously. Solove (2021) contends that reliance on notice-and-consent models obscures structural power imbalances and fails to protect individuals from systemic harms arising from large-scale data processing. In cybersecurity contexts, users often have no practical ability to refuse data collection without forfeiting access to essential digital services.

Automated decision-making further complicates privacy governance. Decisions generated through AI models may produce significant effects—such as account suspension, heightened monitoring, or risk classification—without human review. Legal scholars have warned that such practices undermine procedural fairness and due process, particularly where individuals lack mechanisms to contest or understand automated outcomes (Citron & Pasquale, 2014).

European legal scholarship has been at the forefront of analysing AI governance, particularly following the implementation of the GDPR and the proposal of the EU Artificial Intelligence Act. Commentators widely regard the GDPR as a landmark instrument that reframed data protection as a fundamental rights issue rather than a mere consumer protection concern (Kuner, 2020).

Article 22 of the GDPR, which restricts decisions based solely on automated processing, has attracted significant academic attention. Scholars argue that this provision reflects a normative commitment to human oversight and dignity in algorithmic decision-making, even while its scope and exceptions remain contested (Wachter, Mittelstadt, & Floridi, 2017). In cybersecurity contexts, Article 22 is particularly relevant where automated threat responses produce legal or similarly significant effects for individuals.

The proposed EU Artificial Intelligence Act has further deepened scholarly debate. Legal analyses emphasise its risk-based classification system, under which AI systems used in critical infrastructure and security are typically designated as "high-risk" (Veale & Borgesius, 2021). This designation triggers obligations relating to risk management, transparency, human oversight, and post-market monitoring.

Importantly, EU scholars highlight that the AI Act shifts regulatory focus from *outcomes* to *system design and governance*. By embedding accountability obligations throughout the AI lifecycle, the EU model seeks to prevent rights violations before they occur, rather than relying solely on ex post remedies (Hacker et al., 2020).

Indian legal literature on data protection has largely developed in response to constitutional jurisprudence rather than technological innovation. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* catalysed extensive academic engagement with proportionality, necessity, and procedural safeguards in data processing.

Scholars examining the DPDP Act, 2023 generally acknowledge it as a significant legislative milestone but remain critical of its limitations. Bhatia (2023) argues that the Act's broad exemptions for state processing risk diluting constitutional privacy guarantees, particularly in surveillance-heavy domains such as cybersecurity. Others highlight the absence of explicit provisions addressing automated decision-making, algorithmic transparency, or AI-specific accountability (Ramanathan, 2024).

Cybersecurity scholarship in India has traditionally focused on cybercrime, critical infrastructure protection, and national security. The role of AI in reshaping cybersecurity governance has received comparatively limited attention. Where addressed, scholars often note the regulatory vacuum surrounding autonomous security systems and the potential for rights erosion in the absence of clear legal standards (Choudhary & Singh, 2022).

Research Methodology

This study adopts a doctrinal legal research methodology, supplemented by comparative legal analysis, aligning with the approach outlined in the abstract. Doctrinal research is suited to this inquiry as it evaluates the normative adequacy of existing legal frameworks governing AI-enabled cybersecurity systems rather than measuring empirical outcomes. Primary sources include the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, relevant subordinate legislation, and constitutional jurisprudence on privacy and surveillance. Judicial decisions on informational privacy, proportionality, and state surveillance provide constitutional benchmarks for assessing regulatory adequacy. The comparative component draws on the EU General Data Protection Regulation and the EU Artificial Intelligence Act as reference frameworks, using a functional rather than transplantative comparison to illustrate regulatory design for AI-specific risks in cybersecurity. This approach identifies governance gaps in Indian law while considering India's constitutional structure, institutional capacity, and developmental priorities. Secondary sources comprise peer-reviewed literature, policy papers, and regulatory commentary on AI governance, cybersecurity, and privacy. The analysis is evaluative and normative, examining whether Indian legal norms adequately address AI autonomy, continuous surveillance, and automated decision-making in cybersecurity operations.

Indian Legal Framework Governing AI- enabled Cybersecurity

The Information Technology Act, 2000 and AI-Enabled Cybersecurity

The Information Technology Act, 2000 constitutes the foundational statute governing cybersecurity in India. Enacted at a time when digital governance was nascent, the Act primarily addresses electronic transactions, cyber offences, and intermediary liability. Cybersecurity obligations under the Act are framed largely in terms of *due diligence*, *reasonable security practices*, and *incident response*.

Section 43A of the Act imposes liability on body corporates for failure to implement reasonable security practices resulting in wrongful loss or gain. While this provision indirectly relates to data security, it presumes a model of human oversight and organisational control. AI-enabled cybersecurity systems, which operate through self-learning algorithms and autonomous threat responses, do not fit neatly within this framework. The Act does not address questions such as whether an autonomous system's erroneous decision constitutes a failure of due diligence, or how liability should be apportioned between system developers and deployers.

Similarly, institutional mechanisms such as CERT-In are designed to coordinate responses to cybersecurity incidents rather than to regulate the design, deployment, or governance of AI-driven security architectures. Recent directions issued by CERT-In mandate reporting of cyber incidents and data retention obligations but do not differentiate between human-operated and AI-enabled systems. This regulatory silence reinforces a reactive rather than preventive approach to AI-related risks.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents a significant legislative development in India's privacy landscape. The Act establishes a rights-based framework governing the processing of digital personal data, imposing obligations on data fiduciaries and granting enforceable rights to data principals. However, its relevance to AI-enabled cybersecurity is both substantial and limited.

On the one hand, the Act introduces core principles such as lawful purpose, consent, data minimisation, and accountability. These principles apply to cybersecurity systems insofar as they involve the processing of personal data. In theory, AI-enabled monitoring and threat detection activities must therefore comply with consent requirements and purpose limitations.

On the other hand, the Act does not explicitly address automated decision-making or profiling, concepts central to AI-driven cybersecurity. Unlike the GDPR, which contains specific provisions restricting decisions based solely on automated processing, the DPDP Act remains silent on whether individuals have rights to explanation, human review, or contestation of automated cybersecurity decisions.

This silence is particularly problematic in contexts where AI systems autonomously flag users, restrict access, or escalate surveillance measures. In the absence of statutory safeguards, such decisions risk operating beyond meaningful legal scrutiny.

A further limitation of the DPDP Act lies in its broad exemptions for state processing of personal data. The Act permits exemptions where processing is necessary for reasons including national security, public order, and prevention of offences. While such exemptions are not uncommon in data protection regimes, their breadth and lack of procedural safeguards raise concerns when combined with AI-enabled cybersecurity surveillance.

AI systems enable surveillance at unprecedented scale and granularity. When deployed by state agencies under broadly framed exemptions, they risk facilitating continuous monitoring without proportionality assessments or independent oversight. Indian constitutional jurisprudence has emphasised that privacy intrusions must satisfy tests of legality, necessity, and proportionality. However, the DPDP Act does not clearly operationalise these standards in the context of automated surveillance.

The result is a regulatory asymmetry while constitutional doctrine recognises privacy as a fundamental right, statutory frameworks governing AI-driven cybersecurity do not adequately translate this recognition into enforceable safeguards.

Perhaps the most significant governance gap in Indian law concerns accountability and liability for AI-enabled cybersecurity systems. Existing frameworks assume identifiable human decision-makers and linear chains of responsibility. AI systems, by contrast, operate through distributed decision-making involving developers, vendors, deployers, and end-users.

From a rule-of-law perspective, accountability deficits erode trust in digital governance and weaken the legitimacy of cybersecurity interventions. Without explicit legal standards addressing AI autonomy, Indian cybersecurity governance risks becoming functionally opaque and normatively under-regulated.

Comparative Analysis: The European Union Framework

The European Union's General Data Protection Regulation (GDPR) represents one of the most comprehensive and rights-oriented data protection regimes globally. Unlike technology-neutral frameworks that merely articulate general principles, the GDPR expressly anticipates the risks posed by automated processing and profiling, making it particularly relevant to AI-enabled cybersecurity systems.

Article 22 of the GDPR grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, where such decisions produce legal effects or similarly significant consequences. In cybersecurity contexts, this provision applies where automated systems trigger outcomes such as denial of access to digital services, suspension of accounts, or classification of users as security risks. Legal scholarship has noted that these effects, although often framed as technical security measures, can materially impact individuals' rights and interests (Wachter et al., 2017).

While Article 22 allows exceptions for reasons such as public security, these exceptions are subject to safeguards including the right to human intervention, the ability to express one's point of view, and the right to contest decisions. This framework reflects a normative commitment to preserving human agency and procedural fairness even in high-security environments. In contrast to Indian law, the GDPR embeds these safeguards directly into statutory text rather than leaving them to discretionary policy.

The EU Artificial Intelligence Act (AI Act) builds upon the GDPR's rights-based foundation by introducing a comprehensive, risk-based regulatory model for AI systems. The Act classifies AI applications into categories ranging from minimal risk to unacceptable risk, with corresponding regulatory obligations. AI systems deployed in cybersecurity and critical infrastructure protection are frequently categorised as high-risk, given their potential impact on fundamental rights and societal interests.

For high-risk AI systems, the AI Act imposes extensive obligations on both providers and deployers. These include requirements relating to data governance, bias mitigation, risk management, technical documentation, record-keeping, and post-deployment monitoring. Importantly, the Act mandates human oversight mechanisms designed to ensure that automated systems remain subject to meaningful control and intervention.

From a cybersecurity perspective, this framework recognises that security systems are not value-neutral. By subjecting them to heightened regulatory scrutiny, the EU acknowledges that AI-enabled cybersecurity can itself become a source of rights infringement if left unchecked.

A central contribution of the AI Act lies in its approach to accountability. The Act distinguishes clearly between different actors within the AI ecosystem, including system providers, deployers, and users. Each category bears specific obligations, reflecting their respective roles in design, implementation, and operation.

This allocation of responsibility addresses a key challenge posed by AI autonomy: the diffusion of decision-making authority. By imposing ex ante obligations throughout the AI lifecycle, the EU framework reduces reliance on ex post liability and strengthens preventive governance. Scholars have emphasised that this model enhances legal certainty and facilitates enforcement, particularly in complex technological environments (Hacker et al., 2020).

In contrast, Indian law lacks comparable distinctions or lifecycle-based obligations. The absence of clear responsibility allocation in India exacerbates accountability gaps and weakens both deterrence and redress mechanisms in AI-enabled cybersecurity contexts.

European jurisprudence has consistently emphasised proportionality as a cornerstone of data protection and surveillance regulation. The GDPR operationalises this principle through requirements of data minimisation, purpose limitation, and necessity. The AI Act further reinforces proportionality by calibrating regulatory obligations to the level of risk posed by specific AI applications.

In cybersecurity contexts, this approach ensures that surveillance measures are not only effective but also legally justified and rights-respecting. Automated monitoring must be demonstrably necessary and proportionate to identified risks, and safeguards must be embedded to prevent function creep and overreach.

This stands in contrast to India's regulatory approach, where proportionality standards are primarily articulated through constitutional jurisprudence rather than detailed statutory provisions. The EU model illustrates how proportionality can be operationalised through concrete regulatory design rather than abstract principles alone.

The EU framework demonstrates that effective cybersecurity governance need not come at the expense of fundamental rights. By explicitly addressing AI autonomy, automated decision-making, and accountability, the GDPR and AI Act provide a structured approach to managing the risks inherent in AI-enabled cybersecurity systems.

For comparative purposes, the EU model serves not as a blueprint but as a normative reference point. It illustrates

how legal frameworks can move beyond technology-neutrality to engage directly with AI-specific challenges. This comparative insight is particularly valuable for India, where rapid technological adoption has outpaced regulatory innovation.

Results and Findings

The findings directly address the research question concerning the adequacy of India's regulatory framework.

Structural Inadequacy of Technology-Neutral Regulation

The first major finding of this study is that India's technology-neutral regulatory approach is structurally inadequate to address the governance challenges posed by AI-enabled cybersecurity systems. While flexibility is often cited as a virtue of technology-neutral legislation, the analysis demonstrates that such neutrality becomes a limitation when regulatory frameworks fail to engage with the distinctive characteristics of AI, particularly autonomy, opacity, and scalability.

Indian cybersecurity and data protection laws assume that security decisions are either directly made or meaningfully supervised by human actors. AI-enabled cybersecurity systems disrupt this assumption by generating decisions through probabilistic models that evolve dynamically over time. The absence of AI-specific provisions results in regulatory ambiguity regarding the legality and oversight of autonomous cybersecurity actions, thereby weakening the protective capacity of existing legal norms.

Erosion of Meaningful Consent and Informational Self-Determination

The second finding concerns the erosion of meaningful consent in AI-driven cybersecurity environments. Continuous data monitoring, behavioural analysis, and real-time threat detection undermine traditional consent-based models of data protection. Individuals are rarely aware of the extent, frequency, or nature of data processing undertaken by AI-enabled security systems.

Under the DPDP Act, consent remains a central legal basis for data processing. However, in cybersecurity contexts, consent is often implied, bundled, or effectively coerced through mandatory system use. This disconnect between doctrinal consent requirements and technological reality weakens the principle of informational self-determination and risks reducing consent to a formalistic compliance mechanism rather than a substantive safeguard.

Accountability and Liability Gaps in Autonomous Cybersecurity Systems

A third critical finding relates to accountability and liability. Indian law provides no coherent framework for attributing responsibility when AI-enabled cybersecurity systems cause harm. Where automated systems misclassify individuals, trigger excessive surveillance, or generate false positives, affected persons face significant barriers in identifying responsible actors and seeking remedies.

Proportionality Deficits in AI-Enabled Surveillance

The study further finds that AI-enabled cybersecurity surveillance risks violating proportionality standards central to constitutional privacy jurisprudence in India. Automated systems enable persistent, large-scale monitoring that exceeds the scope of traditional surveillance mechanisms.

While Indian constitutional law mandates that privacy intrusions satisfy tests of legality, necessity, and proportionality, these standards are not adequately operationalised in statutory cybersecurity regulation. The lack of clear thresholds, oversight mechanisms, and ex ante impact assessments allows AI-driven surveillance to expand without rigorous rights-based scrutiny.

Comparative Superiority of the EU Risk-Based Model

Finally, the comparative analysis reveals the normative and regulatory advantages of the EU's risk-based approach. By explicitly identifying high-risk AI systems and imposing heightened obligations, the EU framework aligns cybersecurity governance with fundamental rights protection.

The EU model demonstrates that accountability, transparency, and security can coexist within a coherent regulatory structure. This finding supports the argument that India's current framework requires recalibration to address AI-specific risks without undermining cybersecurity objectives.

Discussion, Normative Implications, Conclusion, and Reform Proposals

The findings of this study underscore a fundamental tension at the heart of AI-enabled cybersecurity governance: the need to secure digital systems against increasingly sophisticated threats while preserving constitutional and human rights protections. AI technologies magnify this tension by enabling security measures that are continuous, predictive, and autonomous. While such capabilities enhance operational effectiveness, they also expand the scope and intensity of surveillance in ways that strain existing legal frameworks.

In the Indian context, this tension is exacerbated by a regulatory architecture that prioritises functional flexibility over normative clarity. The technology-neutral orientation of the IT Act and the DPDP Act reflects an understandable legislative caution in the face of rapid technological change. However, neutrality becomes normatively problematic when it obscures the specific risks associated with AI autonomy. As the analysis demonstrates, AI-enabled cybersecurity systems are not merely faster or more efficient versions of traditional tools; they represent a qualitative transformation in decision-making authority and surveillance capacity.

The absence of explicit safeguards governing automated cybersecurity decisions creates a governance vacuum in which security practices may evolve without sufficient legal constraint. This raises concerns not only for individual privacy but also for democratic accountability. Cybersecurity systems increasingly function as quasi-regulatory mechanisms, shaping access, behaviour, and risk classification without transparent legal authorisation.

From a rule-of-law perspective, such developments demand closer scrutiny rather than regulatory deference.

The deployment of AI-enabled cybersecurity systems has significant normative implications for constitutional governance in India. The recognition of privacy as a fundamental right imposes substantive obligations on the state to ensure that data processing practices respect legality, necessity, and proportionality. However, these obligations are difficult to enforce where statutory frameworks fail to articulate clear standards for AI-driven surveillance and decision-making.

One key implication concerns the transformation of consent. In AI-driven environments, consent loses its traditional role as a meaningful expression of individual autonomy. Where cybersecurity monitoring is continuous and embedded in system architecture, individuals cannot realistically opt out or negotiate terms. This necessitates a shift away from consent-centric models towards accountability- and design-based safeguards, such as privacy-by-design and purpose limitation enforced through regulatory oversight.

Another implication relates to liability and redress. Effective rights protection requires that individuals have access to remedies when harm occurs. The diffusion of responsibility inherent in AI ecosystems undermines this requirement unless law intervenes to allocate responsibility explicitly. Without such intervention, AI-enabled cybersecurity risks creating zones of legal irresponsibility inconsistent with constitutional principles.

Reform Proposals: Towards AI-Sensitive Cybersecurity Governance in India

Drawing on comparative insights from the European Union, this paper proposes targeted reforms aimed at strengthening India's regulatory response to AI-enabled cybersecurity while respecting domestic constitutional and institutional realities.

First, Indian law should incorporate AI-specific regulatory recognition within cybersecurity and data protection frameworks. This does not require exhaustive technological prescription but should include statutory acknowledgment of automated decision-making, profiling, and AI autonomy, particularly in high-risk security contexts.

Second, a risk-based governance model should be adopted for AI-enabled cybersecurity systems. Systems deployed in critical infrastructure protection, mass surveillance, or law enforcement should be subject to heightened obligations, including impact assessments, human oversight requirements, and periodic audits. Such a model would align regulatory intensity with potential rights impact.

Third, the legal framework should establish clear accountability and liability allocation across the AI lifecycle. Developers, deployers, and operators of AI-enabled cybersecurity systems should bear differentiated responsibilities based on their control and influence over system design and deployment. This would enhance legal certainty and facilitate effective enforcement.

Fourth, procedural safeguards against automated decision-making should be introduced. Individuals affected by significant automated cybersecurity decisions should have access to explanations, human review, and grievance redress mechanisms. These safeguards would operationalise constitutional principles of fairness and due process in algorithmic environments.

Finally, India should strengthen institutional oversight mechanisms, including the role of data protection authorities and cybersecurity regulators, to ensure coordinated governance of AI-enabled security systems. Regulatory capacity-building will be essential to translating legal norms into effective practice.

Conclusion

This paper has examined the adequacy of India's privacy and data protection regime in regulating AI-enabled cybersecurity systems through a doctrinal and comparative legal analysis. The study demonstrates that while India has made important strides in data protection and cybersecurity regulation, its existing frameworks remain ill-equipped to address the distinctive challenges posed by autonomous AI-driven security technologies.

By contrast, the European Union's risk-based approach under the GDPR and the Artificial Intelligence Act illustrates how legal systems can engage directly with AI autonomy, accountability, and rights protection without compromising security objectives. The comparative analysis highlights the limitations of technology-neutral regulation and underscores the need for AI-sensitive governance models.

Ultimately, effective cybersecurity governance in the age of AI requires a recalibration of legal principles governing consent, proportionality, and liability. By adopting targeted reforms grounded in constitutional values and informed by global best practices, India can strengthen its cybersecurity framework while safeguarding fundamental rights. Such an approach is essential not only for protecting individual privacy but also for maintaining public trust and legitimacy in digital governance

.

REFERENCES

1. Bhatia, G. (2023). Privacy, proportionality, and the limits of data protection reform in India. *Indian Law Review*, 7(2), 145–162.
2. Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.
3. Choudhary, R., & Singh, P. (2022). Cybersecurity regulation in India: Emerging challenges and legal responses. *National Law School Journal*, 34, 89–112.
4. Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1–33.

5. DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch*. Yale University Press.
6. Hacker, P., Engel, A., & Mauer, M. (2020). Regulating artificial intelligence: Legal frameworks and risk-based approaches. *Columbia Journal of European Law*, 26(3), 543–594.
7. Kuner, C. (2020). The GDPR as a global data protection standard. *European Data Protection Law Review*, 6(2), 137–148.
8. Solove, D. J. (2021). *Understanding privacy* (2nd ed.). Harvard University Press.
9. Veale, M., & Borgesius, F. Z. (2021). Demystifying the EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112.
10. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation does not exist in the GDPR. *International Data Privacy Law*, 7(2), 76–99.
11. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.
12. Bhatia, G. (2023). *Privacy, proportionality, and the limits of data protection reform in India*. Indian Law Review, 7(2), 145–162. https://doi.org/10.1080/24730580.2023.2194821
13. European Commission. (2024). *Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
14. European Union Agency for Cybersecurity (ENISA). (2023). *Artificial intelligence cybersecurity challenges*. ENISA.
15. Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2023). How to design AI for social good: Seven essential factors. Science and Engineering Ethics, 29(1), 1–23. https://doi.org/10.1007/s11948-022-00380-y
16. MeitY (Ministry of Electronics and Information Technology). (2023). *IndiaAI mission document*. Government of India.
17. NITI Aayog. (2024). *Responsible AI for all: National strategy and governance framework*. Government of India.
18. Organisation for Economic Co-operation and Development (OECD). (2022). *AI and cybersecurity: Opportunities and challenges*. OECD Publishing. https://doi.org/10.1787/7c1f0b0d-en
19. Ramanathan, U. (2024). Automated decision-making and the Digital Personal Data Protection Act, 2023: Missing links in India's AI governance. NUJS Law Review, 17(1), 1–26.
20. Solove, D. J. (2024). *Privacy harms in an age of automation*. California Law Review, 112(1), 1–54.
Veale, M., & Borgesius, F. Z. (2023). Demystifying the draft EU Artificial Intelligence Act. Computer Law Review International, 24(4), 97–112. https://doi.org/10.9785/cri-2023-240402