LEGAL CHALLENGES OF REGULATING AI AND ML IN CYBERSECURITY: EXPLORING HOW CYBER LAW CAN KEEP UP WITH ADVANCEMENTS IN AI AND ML

Navya Jha*

ABSTRACT

The rapid evolution of Artificial Intelligence (AI) and Machine Learning (ML) has significantly transformed cybersecurity by enabling automated threat detection, predictive analytics, and real-time response mechanisms. As cyber threats grow in complexity and scale, AI-driven cybersecurity systems have become indispensable tools for safeguarding digital infrastructure. However, the increasing reliance on autonomous and adaptive technologies has raised critical legal, ethical, and regulatory concerns that existing cyber laws struggle to address. This paper examines the legal challenges associated with regulating AI and ML in cybersecurity, with particular emphasis on accountability, transparency, data protection, jurisdiction, and fundamental rights. It analyses the adequacy of existing legal frameworks in India, including the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, in governing AI-driven cybersecurity systems. The study further undertakes a comparative analysis of international regulatory approaches, particularly those adopted by the European Union, the United States, and China, to identify emerging global trends and best practices. Through doctrinal and analytical research, the paper highlights significant regulatory gaps arising from autonomous decision-making, algorithmic opacity, and cross-border data processing. It also examines judicial approaches to privacy, surveillance, and automated decision-making to assess how constitutional principles may guide the regulation of AI-based cybersecurity tools. The paper concludes that while AI and ML enhance cybersecurity effectiveness, their lawful deployment requires a balanced regulatory approach that promotes innovation while safeguarding individual rights and national security. It argues for the

*BA LLB, THIRD YEAR, DES SHRI NAVALMAL FIRODIA LAW COLLEGE, PUNE.

development of risk-based, transparent, and accountable legal frameworks capable of keeping pace with rapid technological advancements in AI and ML.

Keywords: AI, Machine Learning, Cybersecurity, Cyber Law, Data Protection.

INTRODUCTION

In today's interconnected world, the proliferation of technology has revolutionised the way we live, work, and communicate and how the world operates.[1] During the current digital age, the rise of cyber threats has reached unprecedented levels, with issues such as data breaches, ransomware attacks and sophisticated hacking techniques becoming increasingly common.

In response to these challenges, AI and ML have emerged as powerful tools in the world of cybersecurity. They have introduced a paradigm shift in the way cybersecurity is approached. By utilising AI's power, systems can mimic human-like intelligence processes, including learning, reasoning, and decision-making. ML, a subset of AI, allows systems to learn from data, recognise patterns, and make decisions with little assistance from humans. These technologies are not only improving cybersecurity systems' capabilities but also offering a proactive strategy for spotting and reducing threats before they have a chance to do serious damage.[2] As a result, AI-driven cybersecurity solutions are now widely deployed for intrusion detection, malware identification, fraud prevention, and automated threat response mechanisms.

The ability of AI and ML systems to analyse vast amounts of data, detect anomalies, and predict potential cyber threats with remarkable speed and accuracy. AI- motivated solutions like intrusion detection systems, automated threat intelligence, and adaptive security measures are now essential components of modern cybersecurity strategies to prevent potential substantial harm beforehand. However, integrating AI and ML into cybersecurity practices comes with its own set of legal complexities. The dynamic and autonomous nature of these technologies, currently present in traditional tools, AI systems can evolve and make decisions

[1] Babajide Tatalope Familoni, 'Cybersecurity Challenges in the Age of AI: Theoretical Approaches and Practical Solutions' (2024) 5(3*) Computer Science and IT Research Journal* https://fepbl.com/index.php/csitrj/article/view/930 accessed 14 October 2025.

[2] Ayush Trivedi and Krishnappa Jangal, 'Artificial Intelligence and Machine Learning in Cybersecurity' *Arabian Agriculture Services Company (ARASCO)* https://www.researchgate.net/publication/383455388_Artificial_Intelligence_and_Machine_Learning_in_Cybersecurit accessed 9 February 2025.

on their own, often without direct human oversight. This raises questions about accountability, liability, and transparency.

Furthermore, hackers are increasingly using AI to automate attacks, develop sophisticated phishing schemes, and even create malware that can evade traditional detection methods. The dual use of the nature of AI and ML within cybersecurity highlights the significance of developing these technologies within cybersecurity to stay ahead of malicious actors. AI and ML are not only improving defensive capabilities but are also being used offensively by cybercriminals.[3]

Concerns regarding data security and privacy are also raised due to the application of AI and ML. These technologies frequently require access to private information about individuals and organisations, which may violate privacy laws in various countries. As data flows across borders, the global dimension of cyber risks adds another level of complexity, making compliance and enforcement more difficult.

The regulation of AI and ML is also heavily influenced by ethical considerations. There is a risk of adversarial attacks, in which malevolent actors manipulate AI algorithms to bypass security measures, which further complicates the use of these technologies. At last, there is the possibility that AI systems will generate false positives, in which legitimate activities are flagged as threats, and false negatives, in which real threats go undetected, and the potential risk of excessive surveillance highlights the need for a delicate balance between innovation and protecting fundamental rights. As AI systems continue to advance, the absence of clear regulatory frameworks poses risks not only to individuals and organisations but also to national and global security.[4]

Despite the growing reliance on AI and ML in cybersecurity, regulatory responses have largely remained fragmented and reactive. In the Indian context, existing cyber laws were not designed to address autonomous decision-making systems or algorithmic governance. The absence of a comprehensive legal framework specifically tailored to AI-driven cybersecurity exposes significant regulatory gaps that may compromise both individual rights and national security interests.

[3] ibid
[4] ibid 1 2

Against this backdrop, this paper critically examines the legal challenges associated with regulating Artificial Intelligence and Machine Learning in cybersecurity. It analyses the adequacy of existing cyber laws in addressing issues of accountability, data protection, and jurisdiction, and undertakes a comparative assessment of international regulatory approaches. The research aims to investigate the evolution of cyber law in response to the swift progressions in artificial intelligence (AI) and machine learning (ML), while safeguarding transparency, accountability, and fundamental rights.

CONCEPTUAL FRAMEWORK

Artificial Intelligence and Machine Learning: AI refers to computer systems that can perform tasks requiring human-like intelligence, such as problem-solving, decision-making, and pattern recognition. It can also automate security processes, detect anomalies, and predict threats. AI has evolved into a foundation of computer science, focusing on simulating human cognitive processes through complex mathematical algorithms. It combines elements from various domains to create machines that can learn, reason, and make decisions based on the data they process and includes the imitation of human thought and behaviour in robots.[5] AI technology can be used to provide a variety of services that range across a wide spectrum from education to business and marketing.

ML is a subset of AI that focuses on self-learning algorithms that improve over time without explicit programming. Arthur Samuel, one of the pioneers in AI who popularised the term "machine learning", defined ML as the field of study that gives computers the ability to learn without being explicitly programmed.[6] ML focuses on self- learning algorithms that improve over time without explicit programming, which analyse security data, recognise attack patterns, and evolve to detect new threats. It is a system that enables systems to learn from data and make decisions without having to be programmed specifically for every task. Instead of following set guidelines, they can learn on their own from data, which makes the process more

[5] Aya H. Salem,Safaa M. Azzam,O.E.Emmam,Amr A.Abhony, ' Advancing Cybersecurity: a comprehensive review of AI-Driven detection techniques' *Journal of Big Data* < https://link.springer.com/article/10.1186/s40537-024-00957-y> assessed 12 January 2026.

[6] Ravi Sen, Gregory Heim, Qilong Zhu, ' Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunitiesfor MIS Academics' 51 *Communications of the associations for Information Systems*< https://aisel.aisnet.org/cais/vol51/iss1/28/> assessed on 12 January 2026.

efficient and less prone to errors. This is especially used in cybersecurity, given how dynamic the nature of cyber threats is, which are difficult to detect through conventional means.[7]

While AI represents the broader concept of intelligent machines, ML provides the technical foundation through which such intelligence is operationalised. AI systems may incorporate multiple techniques, including natural language processing and expert systems, whereas ML specifically relies on statistical models and data-driven learning. This distinction is important in understanding how these technologies function within cybersecurity frameworks and why they pose unique regulatory challenges. The increasing reliance on AI and ML in digital security environments has therefore transformed both the technical and legal dimensions of cybersecurity.

Types of Machine Learning Relevant to Cybersecurity: Machine Learning techniques used in cybersecurity can broadly be categorised into supervised learning, unsupervised learning, and reinforcement learning. Each of these approaches plays a distinct role in identifying and responding to cyber threats.

Supervised learning involves training algorithms on labelled datasets, where the system is provided with examples of both legitimate and malicious activities. By learning from known patterns, supervised ML models are widely used in applications such as malware detection, spam filtering, and fraud identification. These systems rely on historical data to classify new inputs, making them effective where threat patterns are well documented. They are used in speech recognition, weather forecasting, fraud and email spam detection, etc.[8]

Unsupervised learning, on the other hand, operates on unlabelled data and focuses on identifying anomalies or unusual patterns within datasets. In cybersecurity, this approach is particularly useful for detecting novel or previously unknown attacks. By establishing a baseline of normal system behaviour, unsupervised ML models can flag deviations that may indicate potential security breaches. This method is especially relevant in addressing zero-day vulnerabilities and emerging cyber threats.

[7] 'Machine Learning in Cybersecurity: Applicatrions and challenges(Geeks for Geeks, 2025) < https://www.geeksforgeeks.org/blogs/ml-in-cyber-security/> asseed 12 January 2026.
[8] 'Types of Machine Learning' (Geeks for geeks) < https://www.geeksforgeeks.org/machine-learning/types-of-machine-learning/> assessed on 12 January 2026.

Reinforcement learning differs from the previous approaches by enabling systems to learn through continuous interaction with their environment. In this model, algorithms make decisions and receive feedback in the form of rewards or penalties based on their actions. In cybersecurity, reinforcement learning is increasingly explored for automated response mechanisms, where systems adapt their defensive strategies in real time. While promising, this form of ML also raises concerns regarding autonomous decision-making and accountability, issues that have significant legal implications and are examined in later sections of this paper.[9]

Role of AI and ML in Cybersecurity: Artificial Intelligence and Machine Learning play a pivotal role in strengthening modern cybersecurity systems by enabling automated, adaptive, and predictive security mechanisms. Traditional cybersecurity tools largely rely on predefined rules and signature-based detection methods, which are often inadequate in addressing rapidly evolving cyber threats. AI and ML, by contrast, allow systems to continuously learn from data and adapt to new attack patterns, making them particularly effective in dynamic threat environments.

One of the primary roles of AI and ML is regarding threat detection and prevention. Machine learning algorithms are widely used to analyse network traffic, system logs, and user behaviour in order to identify suspicious activities. By establishing behavioural baselines, AI-driven systems can detect anomalies that may indicate malware infections, unauthorised access, or insider threats. This capability enables early identification of cyber incidents, thereby reducing potential damage.[10]

AI and ML are also extensively used in intrusion detection and prevention systems. These systems monitor network activities in real time and employ predictive analytics to identify potential intrusions before they are fully executed. Unlike conventional intrusion detection systems, AI-driven models can adapt to novel attack techniques and reduce reliance on static rule sets. This adaptability significantly enhances the effectiveness of cybersecurity defences.

Another important role of AI and ML lies in malware detection and analysis. Advanced ML models are capable of identifying malicious software based on behavioural characteristics rather than known signatures. This approach is particularly useful in detecting zero-day attacks and polymorphic malware that frequently evade traditional detection methods. AI-powered

[9] ibid
[10] Trivedi and Jangal (n 2)

malware analysis tools can also automate the classification and prioritisation of threats, enabling faster response times. Anomaly detection is most useful to identify zero-day exploits and advanced persistent threats (APTs) that may evade traditional signature-based detection systems.[11]

In addition to detection, AI and ML facilitate automated response mechanisms in cybersecurity systems. Automated incident response tools can isolate compromised systems, block malicious traffic, and initiate corrective measures with minimal human intervention. While such automation improves efficiency and reduces response time, it also introduces concerns regarding autonomous decision-making and the potential consequences of erroneous actions. These concerns become especially significant when AI-driven responses impact critical infrastructure or essential services.

Overall, the integration of AI and ML into cybersecurity systems has transformed the security landscape by enabling proactive threat management and real-time defence capabilities.

LEGAL FRAMEWORK

Cybersecurity Laws in India: India's cybersecurity framework is primarily governed by the Information Technology Act, 2000 (IT Act), which serves as the foundational legislation regulating electronic records, digital transactions, and cyber offences.[12] Although enacted before the emergence of Artificial Intelligence-driven cybersecurity systems, the IT Act provides the basic legal structure for addressing cyber threats, unauthorised access, data breaches, and misuse of computer resources. Provisions such as Sections 43 and 66 of the Act impose civil and criminal liability for unauthorised access, data damage, and cyber intrusions, which are relevant to cybersecurity operations involving AI-based tools.[13]

In addition to statutory provisions, institutional mechanisms play a significant role in India's cybersecurity governance. The Indian Computer Emergency Response Team (CERT-In), established under Section 70B of the IT Act, functions as the national nodal agency for responding to cybersecurity incidents.[14] CERT-In issues advisories, guidelines, and directions

[11] Sarah Al-Mansoori,Mohamed Ben Salem, ' The role of Artificial Intelligence and Machine learning in shaping the future of cyber security: Trends, Applications and Ethical Considerations' *IJSA* 8 <https://norislab.com/index.php/ijsa/article/view/36 > assessed on 12 January 2026.
[12] Information Technology Act 2000.
[13] Information Technology Act 2000 ss 43, 66.
[14] Information Technology Act 2000 s 70B.

aimed at enhancing cyber resilience across public and private sectors. These directions increasingly apply to organisations deploying advanced cybersecurity technologies, including AI-enabled monitoring and threat detection systems.[15]

India's broader cybersecurity policy framework is supplemented by initiatives such as the National Cyber Security Policy, 2013, which emphasises the protection of critical information infrastructure and capacity building in cybersecurity.[16] While the policy does not explicitly regulate AI or ML-based security systems, its objectives indirectly encompass technologies that enhance threat detection and response. Consequently, AI-driven cybersecurity tools currently operate within a legal framework that was not specifically designed for autonomous or adaptive technologies but is applied through broad and technology-neutral provisions.

Data Protection and Privacy Laws: The use of AI and ML in cybersecurity has significant implications for data protection and privacy, as these systems often rely on continuous access to large volumes of personal and sensitive data. In India, data protection obligations are now primarily governed by the Digital Personal Data Protection Act, 2023 (DPDP Act), which establishes a comprehensive framework for the lawful processing of personal data.[17] The Act introduces key principles such as consent-based processing, purpose limitation, data minimisation, and accountability of data fiduciaries.[18]

AI-driven cybersecurity systems deployed by organisations may qualify as data processing mechanisms under the DPDP Act, thereby subjecting organisations to statutory obligations regarding lawful collection, storage, and use of personal data. Automated monitoring, behavioural analysis, and anomaly detection tools may process personal data without direct user interaction, raising important questions regarding informed consent and proportionality.[19]

Additionally, the DPDP Act provides for cross-border data transfer restrictions, requiring compliance with conditions notified by the Central Government.[20] Given the global nature of cybersecurity operations and cloud-based AI systems, ensuring compliance with cross-border

[15] Indian Computer Emergency Response Team (CERT-In), *Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents* (28 April 2022) https://www.cert-in.org.in/ accessed 13 January 2026.
[16] Ministry of Communications and Information Technology, *National Cyber Security Policy 2013* (Government of India).
[17] Digital Personal Data Protection Act 2023.
[18] Digital Personal Data Protection Act 2023 ss 4–10.
[19] Aadya Kuhar, 'A Comparative Analysis of Data Protection Laws in India, the UK, and the USA: From Consent to Compliance' (2025) 7(3) *International Journal for Multidisciplinary Research*.
[20] Digital Personal Data Protection Act 2023 s 16.

data transfer requirements becomes particularly complex. While the Act does not specifically regulate AI-based decision-making, its broad applicability to personal data processing makes it a central component of the legal framework governing AI-driven cybersecurity in India.

Regulation of Artificial Intelligence in India: India currently does not have a dedicated statute regulating Artificial Intelligence. Instead, AI governance in India has largely evolved through policy initiatives and soft-law frameworks. The National Strategy for Artificial Intelligence, released by NITI Aayog, outlines India's vision for responsible AI development across sectors such as healthcare, agriculture, and governance.[21] While cybersecurity is not addressed extensively, the strategy emphasises ethical AI, accountability, and transparency, which are relevant to AI-based security applications.

Other initiatives, such as discussion papers and advisory frameworks issued by governmental bodies, promote the adoption of AI while recognising the need for risk-based regulation. These policy instruments encourage innovation and self-regulation rather than imposing binding legal obligations. As a result, AI-driven cybersecurity systems operate within a regulatory environment that prioritises flexibility and technological growth but lacks enforceable standards specific to autonomous decision-making systems.

The absence of a comprehensive AI-specific law creates regulatory ambiguity, particularly when AI systems independently analyse data or initiate security responses. In practice, such systems are governed indirectly through existing cyber and data protection laws, which may not fully account for the complexities introduced by autonomous technologies.

International Legal Frameworks Relevant to AI and Cybersecurity: At the international level, several legal and regulatory frameworks influence the governance of AI and cybersecurity. The General Data Protection Regulation (GDPR) of the European Union represents one of the most comprehensive data protection regimes globally.[22] The GDPR contains provisions relating to automated decision-making and profiling, requiring transparency and accountability when personal data is processed through automated systems.[23] These provisions are particularly relevant for AI-driven cybersecurity tools that analyse user behaviour and network activity.

[21] NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India 2018).
[22] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
[23] GDPR art 22.

Similarly, the California Consumer Privacy Act (CCPA) and its subsequent amendments establish data protection obligations for organisations processing personal data of California residents.[24] Although not specific to AI, these laws impact AI-based cybersecurity systems deployed by multinational corporations.

In addition to binding legislation, international organisations such as the OECD and UNESCO have issued principles and guidelines on the ethical use of Artificial Intelligence. These frameworks emphasise human oversight, fairness, accountability, and transparency, providing normative guidance for the development and deployment of AI technologies, including in cybersecurity contexts.[25]

Applicability of Existing Laws to AI-Driven Cybersecurity Systems: The regulation of AI-driven cybersecurity systems currently relies on the interpretation and application of existing cyber and data protection laws. While technology-neutral legal provisions allow for flexible application, they often fail to address the unique challenges posed by autonomous and adaptive systems. Issues such as attribution of responsibility, explainability of AI decisions, and jurisdictional enforcement remain inadequately addressed within current legal frameworks.[26]

Moreover, cybersecurity incidents involving AI-driven systems frequently transcend national boundaries, raising questions of jurisdiction and enforcement. The lack of harmonised international standards further complicates regulatory compliance for organisations operating across multiple jurisdictions.[27] As a result, AI-based cybersecurity tools are regulated through a patchwork of domestic laws, policy guidelines, and international norms.

This legal framework, while providing a foundational level of regulation, reveals significant limitations in addressing the evolving risks associated with AI and ML in cybersecurity. These limitations form the basis for the legal challenges in cybersecurity.

RESEARCH METHODOLOGY

This study adopts a doctrinal and analytical research methodology to examine the legal challenges associated with regulating Artificial Intelligence and Machine Learning in

[24] California Consumer Privacy Act 2018 (Cal Civic Code 1798.100–1798.199).
[25] Organisation for Economic Co-operation and Development (OECD), *Principles on Artificial Intelligence* (2019); UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[26] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
[27] United Nations Office on Drugs and Crime (UNODC), *Cybercrime and Legal Responses* (UNODC 2020).

cybersecurity. The research is primarily based on the analysis of existing legal frameworks, statutory provisions, judicial decisions, policy documents, and scholarly literature relevant to cyber law, data protection, and artificial intelligence.

Secondary sources of data have been utilised for the purpose of this research. These include statutes such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, international legal instruments, regulatory guidelines, reports published by governmental and international organisations, and academic articles from reputed journals. Case laws from Indian and foreign jurisdictions have also been examined to understand the judicial approach towards issues arising from the use of advanced technologies in cybersecurity.

The study employs a comparative approach where necessary to analyse international regulatory practices and assess their relevance to the Indian legal context. Doctrinal analysis has been used to interpret legal provisions and identify regulatory gaps in existing cyber laws. The scope of the research is limited to the legal and regulatory aspects of AI and ML in cybersecurity and does not extend to technical or engineering-based evaluations.

The research is confined to publicly available data and literature. Given the rapidly evolving nature of AI technologies, the study acknowledges that regulatory developments may continue beyond the scope of this research.

LEGAL CHALLENGES IN REGULATING AI AND ML IN CYBERSECURITY

The swift progress of AI and ML is reshaping or transforming cybersecurity, providing both improved defence strategies and emerging cyber threats. The self-governing decision-making brings about important legal, regulatory, and ethical issues that current cybersecurity laws find challenging to tackle. The lack of legal frameworks specifically concerning AI results in regulatory deficiencies, which complicate enforcement and governance. Some legal challenges emerge from the use of AI in cybersecurity, such as a lack of transparency, Autonomous decision-making and liability, AI-powered cyberattacks, and data privacy conflicts. Present regulations, such as GDPR and the US Cybersecurity Framework, do not specifically tackle AI's involvement in cybersecurity. These challenges stem from the evolving nature of AI systems, their reliance on large-scale data processing, and their capacity to make independent decisions without direct human intervention.

Accountability and Liability: The adoption of AI and ML in cybersecurity has led to many serious questions raised related to the accountability and liability section, where AI-driven systems cause harm. Unlike traditional software, where legal frameworks are premised on the assumption that human actors exercise control over decision-making processes, the current software makes autonomous decisions which evolve and create unpredictable results, making it hard to assign legal responsibility when cybersecurity tools fail or make wrong decisions.

In cases where an AI-driven cybersecurity tool fails to detect a cyber-attack or wrongly flags legitimate activity as malicious, questions arise as to whether liability should rest with the developer, the deploying organisation, the system operator, or the end user. Existing cyber laws, including the Information Technology Act, 2000, do not provide clear guidance on attributing liability in situations involving autonomous decision-making. This ambiguity undermines legal certainty and complicates the enforcement of accountability mechanisms.[28]

Lack of Transparency and Explainability with Respect to Autonomous Decision-Making Systems: AI and ML systems, particularly those based on complex algorithms, often operate as "black boxes," where decision-making processes are not easily explainable. This lack of transparency poses serious legal concerns, especially in cybersecurity contexts where automated decisions may affect access to services, block user activity, or trigger surveillance mechanisms.

From a legal perspective, the inability to explain how an AI system reached a particular conclusion challenges principles of due process and fairness. Individuals and organisations affected by automated cybersecurity decisions may find it difficult to contest or seek remedies without understanding the underlying logic of the system. The absence of legal standards mandating explainability further exacerbates this issue.

For instance, the range of AI spans across multiple industries, from self-driving cars to robotic process automation, illustrating the flexibility and adaptability of these systems. But these autonomous AI systems introduce complexities due to their ability for independent decision-making. Thus, current legal frameworks find it hard to explain accountability.[29]

[28] 'Autonomous AI Legal Entity Liability' (Aaron Hall Attorney) https://aaronhall.com/artificial-intelligence-liability/ assessed 13 January 2026.
[29] Ibid.

Data Protection and Privacy Concerns: AI-driven cybersecurity systems rely heavily on the continuous collection and analysis of vast volumes of data, including personal and sensitive information. This creates significant challenges in complying with data protection and privacy laws. Automated monitoring, behavioural analysis, and predictive threat detection may involve intrusive data processing practices that raise concerns regarding consent, proportionality, and lawful use of data.

In the Indian context, compliance with the Digital Personal Data Protection Act, 2023, becomes particularly complex when AI systems process data in real time without direct user awareness. Additionally, the cross-border nature of data flows in cybersecurity operations further complicates enforcement, as data may be processed or stored outside national jurisdictions.

The utilisation of large datasets brings up a huge worry about data breaches. If the information used to train AI models is not sufficiently safeguarded, it may become an attractive target for cybercriminals. This can result in incorrect predictions and classifications, ultimately jeopardising the efficacy of the cybersecurity systems. These issues highlight the inadequacy of existing privacy frameworks in addressing the realities of AI-based cybersecurity systems.[30]

Jurisdictional and Cross-Border Challenges: Cybersecurity incidents involving AI-driven systems often transcend national boundaries. In a globalised commercial climate, AI-based cybersecurity tools are frequently deployed through cloud-based infrastructures and operate across multiple jurisdictions. This raises complex questions regarding jurisdiction, applicable law, and enforcement mechanisms.

Existing cyber laws are primarily territorial in nature and may not adequately address transnational cyber incidents involving autonomous systems. The lack of harmonised international legal standards further complicates regulatory compliance and enforcement. As a result, victims of cross-border cyber incidents may face significant barriers in seeking legal remedies. For instance, the GDPR can impose harsh penalties on businesses that improperly handle the data of EU citizens, regardless of their location. The GDPR laws will probably be followed by a firm operating in the EU. [31]

[30] Trivedi and Jangal (n 2)
[31] Shannon Lawson, 'Overcoming Regulatory and Legal Challenges in Cybersecurity' (2025) < https://www.redapt.com/blog/overcoming-regulatory-and-legal-challenges-in-cybersecurity> assessed on 13 January 2026.

Ethical and Bias-Related Challenges: Ethical concerns form an integral part of the legal challenges surrounding AI and ML in cybersecurity. AI systems trained on biased or incomplete datasets may generate discriminatory outcomes, leading to unjustified targeting or exclusion of certain users. In cybersecurity contexts, biased algorithms may disproportionately flag specific behaviours or groups as suspicious, raising concerns regarding fairness and equality. Biased labelling mostly occurs when a programmer labels or categorises data in a manner that reflects their own biases.[32]

Additionally, adversarial attacks—where malicious actors manipulate AI models to bypass security measures—pose further ethical and legal concerns. Such vulnerabilities not only undermine system reliability but also raise questions regarding the duty of care owed by organisations deploying AI-based cybersecurity tools.[33]

Over-Surveillance and Fundamental Rights: The deployment of AI-driven cybersecurity systems has the potential to result in excessive surveillance. Continuous monitoring of user activity, network behaviour, and digital communications may infringe upon fundamental rights such as privacy and freedom of expression. The absence of clear legal safeguards regulating the scope and limits of surveillance exacerbates these risks.

Balancing national security interests with the protection of individual rights remains a significant legal challenge. Without adequate oversight and accountability mechanisms, AI-driven cybersecurity tools may be misused for intrusive monitoring beyond their intended security purposes.[34]

Regulatory Gaps and Lack of AI-Specific Legislation: A fundamental challenge in regulating AI and ML in cybersecurity lies in the absence of comprehensive, AI-specific legislation. Existing cyber and data protection laws were not designed to address autonomous systems capable of learning and evolving. As a result, regulatory responses remain fragmented and reactive, relying on broad interpretations of technology-neutral provisions.

---

[32] Promevo, ‘ AI Legal and regulatory Challenges: Understanding Google’s Commitment’ (1May 2024) < https://promevo.com/blog/ai-legal-and-regulatory-challenges> assessed on 14 January 2026.

[33] Dredeir Roberts,Michael Scott Simon, Davind Flint,Lisa R. Lifschitz,Lois Deborah Mermelstein ‘Big Data, Big Problems; The Legal Challenges of AI driven data analysis’ Business Law Section, American bar Association< https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-april/big-data-big-problems/> assessed on 14 January 2026.

[34] Shari Davidson, ‘ The growth of AI law: Exploring Legal challenges in Artificial Intelligence’ National Law review guest contributor (January 2025) < https://natlawreview.com/article/growth-ai-law-exploring-legal-challenges-artificial-intelligence> assessed on 14 January 2026.

The lack of clear statutory guidance on issues such as autonomous decision-making, liability allocation, and algorithmic accountability highlights the urgent need for regulatory reform. Without such reforms, the legal framework governing AI-driven cybersecurity will continue to lag behind technological advancements.[35]

IMPACT ANALYSIS OF AI AND ML IN CYBERSECURITY

The increasing deployment of Artificial Intelligence and Machine Learning in cybersecurity has had a significant impact on legal systems, regulatory institutions, private organisations, and individual rights. While these technologies have enhanced the efficiency and effectiveness of cyber defence mechanisms, their broader implications reveal complex legal, social, and institutional consequences that warrant careful examination.

Impact on Regulatory and Legal Frameworks: The integration of AI and ML into cybersecurity has exposed the limitations of existing legal frameworks that were designed for human-centric decision-making. Traditional cyber laws rely on concepts such as intent, foreseeability, and direct control, which are difficult to apply to autonomous systems. As a result, regulatory authorities often struggle to interpret and enforce existing laws in cases involving AI-driven cybersecurity incidents.

This technological shift has compelled regulators to rely on broad, technology-neutral provisions, which may offer flexibility but lack precision. The absence of AI-specific statutory guidance has led to regulatory uncertainty, making compliance challenging for organisations and weakening enforcement mechanisms. Consequently, the legal system faces increasing pressure to adapt its conceptual foundations to accommodate algorithmic decision-making. But, countries such as the US advocate for explainability benchmarks for AI cybersecurity models to manage risks related to AI and reduce loss.[36]

Impact on Organisational Accountability and Compliance: For organisations, the adoption of AI-based cybersecurity tools has altered compliance obligations and risk management strategies. Automated threat detection and response systems can significantly reduce response

[35] Saumya Kashyap, Anshika Chandra, ' Cybersecurity and International Law: Exploring Existing Frameworks and the need for new regulations in the Digital Age' E-Justice India (November 2024) < https://www.ejusticeindia.com/cybersecurity-and-international-law-digital-age/> assessed on 14 January 2026.
[36] RSI Security, ' Comparing NIST AI RMF with other AI Risk Management Frameworks' (12 February 2025) < https://blog.rsisecurity.com/comparing-nist-ai-rmf-with-other-ai-risk-management-frameworks/> assessed 16 January 2026.

times and operational costs. However, they also increase dependence on complex technologies whose functioning may not be fully understood by decision-makers.

This reliance complicates internal accountability structures, as organisations may find it difficult to explain or justify automated cybersecurity decisions to regulators, courts, or affected individuals. Additionally, compliance with data protection laws becomes more complex due to continuous data processing, profiling, and cross-border data transfers. Organisations deploying AI-driven cybersecurity tools must therefore balance operational efficiency with heightened legal and compliance risks.[37]

Impact on Individual Rights and Privacy: The use of AI and ML in cybersecurity has a direct impact on individual rights, particularly the right to privacy. Continuous monitoring of digital behaviour, network activity, and communication patterns can lead to intrusive data collection practices. While such surveillance may be justified on security grounds, the lack of clear legal safeguards increases the risk of disproportionate interference with personal freedoms.

AI-driven systems may also generate false positives, where legitimate activities are mistakenly flagged as malicious, resulting in denial of access or unwarranted scrutiny. Conversely, false negatives may allow genuine threats to go undetected, undermining trust in automated security systems. These outcomes highlight the need for transparency, accountability, and effective redress mechanisms to protect individual rights.[38]

Impact on National Security and Critical Infrastructure: At the national level, AI and ML have become integral to the protection of critical infrastructure, including financial systems, energy grids, healthcare networks, and government databases. The ability of AI-driven cybersecurity systems to predict and mitigate large-scale cyber threats enhances national security preparedness.

However, over-reliance on automated systems may also create systemic vulnerabilities. If AI-based cybersecurity tools are compromised through adversarial attacks or technical failures, the resulting impact on critical infrastructure could be severe. The concentration of decision-

[37] Hall, *Autonomous AI Legal Entity Liability* (n 28).
[38] Muhammad Tuhin, 'The Dark of AI: Cybersecurity Threats and Privacy Concerns' (27 May 2024) < https://www.sparity.com/blogs/dark-side-of-ai-in-cybersecurity/> assessed 16 January 2026.

making power in autonomous systems, therefore, necessitates robust oversight and contingency planning to mitigate potential risks.[39]

Impact on the Evolution of Cyber Law and Policy: The widespread adoption of AI and ML in cybersecurity is influencing the evolution of cyber law and policy at both national and international levels. Policymakers are increasingly recognising the need for risk-based and adaptive regulatory approaches that can accommodate technological innovation while safeguarding fundamental rights.

Internationally, the lack of harmonised legal standards has highlighted the importance of cross-border cooperation and shared regulatory principles. The growing influence of AI in cybersecurity is thus shaping future legal discourse, prompting calls for specialised legislation, enhanced regulatory coordination, and ethical governance frameworks. These developments indicate a gradual shift towards more comprehensive and forward-looking cyber law regimes.

JUDICIAL APPROACH TO AI, CYBERSECURITY AND DATA PROTECTION (CASE LAWS)

Judicial interpretation plays a crucial role in shaping the legal understanding of emerging technologies, particularly in areas where legislation has not kept pace with technological advancements. Although Indian courts have not yet directly adjudicated a large number of cases involving Artificial Intelligence-driven cybersecurity systems, judicial decisions relating to data protection, privacy, surveillance, and algorithmic decision-making provide important guidance for regulating AI and ML in cybersecurity contexts.

Right to Privacy and Informational Autonomy: One of the most significant judicial developments influencing AI-driven cybersecurity regulation is the recognition of the right to privacy as a fundamental right. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court of India held that the right to privacy is intrinsic to life and personal liberty under Article 21 of the Constitution.[40] The Court emphasised informational privacy, data protection, and the need for safeguards against arbitrary state action.

[39] 'Paris Call for Trust and Security in Cyberspace', *The 9 Principles* < https://parispeaceforum.org/initiatives/paris-call-for-trust-and-security-in-cyberspace/> assessed 16 January 2026.
[40] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

This judgment has direct implications for AI-based cybersecurity systems that rely on large-scale data collection, monitoring, and profiling. Any deployment of AI-driven surveillance or security mechanisms must satisfy the tests of legality, necessity, and proportionality laid down by the Court.[41] The principles articulated in Puttaswamy provide a constitutional framework for assessing the legality of automated cybersecurity measures that may impact individual privacy.

Automated Decision-Making and Due Process: Judicial concern regarding automated and algorithmic decision-making is evident in cases involving procedural fairness and transparency. In Maneka Gandhi v. Union of India, although not related to technology, the Supreme Court underscored the importance of fairness, reasonableness, and due process in administrative action.[42] These principles become increasingly relevant in the context of AI-driven cybersecurity systems that make automated decisions affecting access to digital services or flag user activities as malicious.

Automated cybersecurity responses that lack human oversight or explainability may conflict with established principles of natural justice. Courts may, therefore, extend existing due process standards to assess the legality of autonomous cybersecurity decisions, particularly where such decisions have adverse consequences for individuals or organisations.[43]

Surveillance and Proportionality: Judicial scrutiny of surveillance mechanisms further informs the regulation of AI-based cybersecurity tools. In People's Union for Civil Liberties (PUCL) v. Union of India, the Supreme Court recognised the need for procedural safeguards to prevent abuse of surveillance powers.[44] The Court emphasised that surveillance must be carried out in accordance with the law and subject to adequate checks and balances.

AI-driven cybersecurity systems that involve continuous monitoring of digital communications or network activity may raise similar concerns. The absence of statutory safeguards governing AI-enabled surveillance could invite judicial intervention, particularly where such systems operate without transparency or accountability.[45]

[41] *Puttaswamy* (n 40).
[42] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
[43] M Sornarajah, 'Due Process, Fairness and Administrative Discretion' (2006) 23 *Journal of Indian Law Institute* 1.
[44] *People's Union for Civil Liberties (PUCL) v Union of India* (1997) 1 SCC 301.
[45] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

International Judicial Perspectives: International judicial decisions also offer valuable insights into the regulation of AI and automated systems. In the European context, courts have increasingly examined the legality of automated data processing under the General Data Protection Regulation (GDPR). Decisions interpreting Article 22 of the GDPR, which deals with automated decision-making, emphasise the importance of human intervention, transparency, and the right to explanation.[46]

Similarly, courts in other jurisdictions have scrutinised algorithmic decision-making in areas such as data profiling and digital surveillance. These judicial approaches reinforce the need for legal safeguards when deploying AI-based cybersecurity systems, particularly in relation to individual rights and accountability.[47]

Emerging Judicial Trends and Future Implications: Although courts have not yet directly addressed AI-driven cybersecurity failures or liability arising from autonomous security systems, existing judicial trends indicate a cautious and rights-oriented approach. Indian courts are likely to rely on constitutional principles, data protection norms, and established doctrines of administrative law to address disputes involving AI-based cybersecurity tools.

As AI technologies become more deeply embedded in cybersecurity infrastructure, judicial interpretation will play an increasingly important role in bridging regulatory gaps. Courts may be required to balance technological innovation with constitutional values, thereby shaping the future legal framework governing AI and ML in cybersecurity. [48]

INTERNATIONAL APPROACH TO REGULATING AI AND ML IN CYBERSECURITY

The regulation of Artificial Intelligence and Machine Learning in cybersecurity has emerged as a significant concern at the international level. Given the transnational nature of cyber threats and the global deployment of AI-driven technologies, several jurisdictions have adopted diverse legal and policy approaches to address the challenges posed by autonomous systems.

[46] Regulation (EU) 2016/679 (General Data Protection Regulation) art 22; *SCHUFA Holding AG v Hessischer Rundfunk* (Case C-634/21) EU:C:2023:344.
[47] *Big Brother Watch v United Kingdom* (2021) 72 EHRR 17.
[48] Frank Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Harvard University Press 2020).

A comparative analysis of these approaches provides valuable insights into potential regulatory models and best practices.

European Union: The European Union has adopted one of the most comprehensive regulatory frameworks addressing data protection and artificial intelligence. The General Data Protection Regulation (GDPR) plays a central role in regulating AI-driven cybersecurity systems that process personal data.[49] Provisions relating to lawfulness of processing, data minimisation, transparency, and automated decision-making under Article 22 have direct relevance to AI-based cybersecurity tools.[50] The GDPR mandates safeguards such as human oversight and the right to explanation, which significantly influence the deployment of automated security systems.

In addition to the GDPR, the European Union has proposed the Artificial Intelligence Act, which adopts a risk-based approach to AI regulation. Under this framework, high-risk AI systems are subject to stringent compliance requirements, including risk assessment, transparency obligations, and accountability measures. AI systems used in critical infrastructure and cybersecurity may fall within this category, thereby subjecting them to enhanced regulatory scrutiny. This approach reflects the EU's emphasis on balancing technological innovation with fundamental rights and public safety. [51]

United States: The regulatory approach to AI and cybersecurity in the United States is largely sector-specific and decentralised. Unlike the European Union, the United States does not have a comprehensive federal law governing AI. Instead, AI-driven cybersecurity systems are regulated through a combination of federal and state laws, industry standards, and policy guidelines.[52]

Data protection obligations are primarily governed by laws such as the California Consumer Privacy Act (CCPA), which imposes transparency and accountability requirements on organisations processing personal data.[53] While the CCPA does not explicitly regulate AI, its provisions impact AI-based cybersecurity tools that involve data profiling and automated analysis. Additionally, federal agencies such as the National Institute of Standards and

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
[50] GDPR arts 5, 22.
[51] European Union Agency for Cybersecurity (ENISA), *Artificial Intelligence and Cybersecurity* (ENISA 2021).
[52] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press 2020).
[53] California Consumer Privacy Act 2018 (Cal civic Code, 1798.100–1798.199).

Technology (NIST) have issued cybersecurity frameworks and AI risk management guidelines that encourage best practices rather than imposing binding legal obligations.[54]

The U.S. approach emphasises innovation, self-regulation, and industry-led standards. While this model promotes technological development, it has been criticised for lacking uniformity and enforceability, particularly in addressing accountability and ethical concerns associated with AI-driven cybersecurity systems.

China: China has adopted a more centralised and state-driven approach to AI regulation. The Chinese government has issued several regulations and guidelines governing the use of AI, data security, and cybersecurity. Laws such as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law establish strict obligations regarding data handling, security, and state oversight.[55]

China's regulatory framework places significant emphasis on national security and state control over digital infrastructure. AI-driven cybersecurity systems are subject to stringent compliance requirements, including security assessments and government supervision. While this approach ensures strong state oversight, it raises concerns regarding individual privacy and freedom of expression. [56]

Lessons for India: The international regulatory landscape highlights the absence of a uniform approach to regulating AI and ML in cybersecurity. Jurisdictions such as the European Union emphasise rights-based and risk-based regulation, while others prioritise innovation or national security. These diverse approaches offer valuable lessons for India.[57]

India may benefit from adopting a hybrid regulatory model that combines technology-neutral legislation with AI-specific safeguards. Incorporating principles such as transparency, accountability, and proportionality, while allowing regulatory flexibility, could help address the unique challenges posed by AI-driven cybersecurity systems. Comparative analysis

[54] National Institute of Standards and Technology (NIST), *AI Risk Management Framework* (NIST 2023).
[55] Cybersecurity Law of the People's Republic of China 2017; Data Security Law of the People's Republic of China 2021; Personal Information Protection Law of the People's Republic of China 2021.
[56] Rogier Creemers, 'China's Social Credit System: An Evolving Practice of Control' (2018) 30 *SSRN Electronic Journal*.
[57] Organisation for Economic Co-operation and Development (OECD), *Principles on Artificial Intelligence* (2019).

underscores the need for India to develop a coherent legal framework that aligns with international best practices while addressing domestic priorities.[58]

FINDINGS

Based on the doctrinal and comparative analysis undertaken in this study, several key findings emerge regarding the regulation of Artificial Intelligence and Machine Learning in cybersecurity.

First, the research finds that while AI and ML have significantly enhanced cybersecurity capabilities through automated threat detection, predictive analytics, and real-time response mechanisms, existing legal frameworks have not evolved at a comparable pace. Most cyber laws, including those in India, were enacted at a time when autonomous and adaptive technologies were not envisaged, resulting in regulatory gaps when applied to AI-driven cybersecurity systems.

Second, the study reveals that existing cyber and data protection laws regulate AI-based cybersecurity tools only indirectly. Technology-neutral provisions allow for flexible interpretation, but they fail to adequately address issues unique to AI systems, such as autonomous decision-making, algorithmic opacity, and continuous learning. As a result, questions of accountability and liability remain unresolved, particularly in cases where AI-driven systems cause harm or fail to prevent cyber incidents.

Third, the findings indicate that data protection and privacy concerns are central to the legal challenges surrounding AI-driven cybersecurity. The extensive collection and processing of personal data by AI-based security systems create compliance difficulties under data protection regimes, especially with respect to consent, proportionality, and cross-border data transfers. The absence of clear safeguards governing automated data processing increases the risk of privacy infringement.

Fourth, the study finds that judicial approaches, both in India and internationally, increasingly emphasise constitutional values such as privacy, due process, and proportionality. Although courts have not yet directly adjudicated disputes involving AI-driven cybersecurity systems,

[58] NITI Aayog, *Responsible AI for All: Approach Document* (Government of India 2021).

existing jurisprudence provides guiding principles that are likely to shape future legal interpretation in this area.

Finally, the comparative analysis demonstrates that international regulatory approaches vary significantly. Jurisdictions such as the European Union have adopted risk-based and rights-oriented frameworks, while others rely on sectoral or policy-based regulation. These variations highlight the lack of harmonised global standards and underscore the need for jurisdiction-specific yet internationally aligned regulatory responses.

Overall, the findings suggest that while AI and ML are indispensable to modern cybersecurity, their effective and lawful deployment requires clearer regulatory guidance, enhanced accountability mechanisms, and a balanced approach that safeguards both security interests and fundamental rights.

SUGGESTIONS AND RECOMMENDATIONS

In light of the findings of this study, several legal and policy-oriented recommendations may be proposed to strengthen the regulation of Artificial Intelligence and Machine Learning in cybersecurity.

First, there is a pressing need to develop a specific regulatory framework for AI-driven cybersecurity systems. While technology-neutral cyber laws provide flexibility, they are insufficient to address challenges arising from autonomous decision-making and algorithmic learning. India should consider adopting a risk-based regulatory approach that categorises AI applications in cybersecurity based on their potential impact on fundamental rights and national security.

Second, clear accountability and liability mechanisms must be established for AI-enabled cybersecurity operations. Legal responsibility should not be obscured by the autonomous nature of AI systems. Organisations deploying AI-based cybersecurity tools must be required to ensure human oversight, explainability of algorithms, and documented audit trails to enable effective attribution of responsibility in cases of failure or misuse.

Third, data protection safeguards must be strengthened to address the extensive data processing involved in AI-driven cybersecurity. Principles such as data minimisation, purpose limitation, and proportionality should be strictly enforced, particularly in relation to automated monitoring

and surveillance mechanisms. Regulatory clarity on cross-border data transfers involving AI security systems is also essential in an increasingly interconnected digital environment.

Fourth, ethical considerations should be formally integrated into cybersecurity governance frameworks. Regulatory guidelines should mandate fairness, transparency, and non-discrimination in the design and deployment of AI systems. Mechanisms to mitigate risks such as algorithmic bias, false positives, and adversarial manipulation must be incorporated at both the development and deployment stages.

Finally, international cooperation is crucial for addressing the transnational nature of cyber threats. India should actively engage in global dialogues and align its regulatory strategy with emerging international standards while retaining flexibility to address domestic cybersecurity needs. Capacity-building initiatives, including judicial and regulatory training on AI-related issues, would further enhance effective enforcement.

CONCLUSION

The rapid integration of Artificial Intelligence and Machine Learning into cybersecurity has transformed the way cyber threats are detected, prevented, and managed. While these technologies offer unprecedented efficiency and predictive capabilities, they also introduce complex legal, ethical, and regulatory challenges that existing cyber laws are ill-equipped to address. The autonomous and adaptive nature of AI systems fundamentally alters traditional notions of control, accountability, and liability within cybersecurity governance.

This study has demonstrated that current legal frameworks, particularly in the Indian context, regulate AI-driven cybersecurity only incidentally and lack provisions specifically tailored to address algorithmic decision-making, transparency, and human oversight. The absence of a comprehensive and coherent regulatory framework risks undermining data protection, privacy rights, and legal certainty, especially as AI systems increasingly operate with minimal human intervention.

Through a comparative analysis of international approaches, the paper highlights that while certain jurisdictions have begun adopting rights-based and risk-oriented regulatory models, there remains a lack of harmonisation in global standards. This fragmentation complicates enforcement and compliance in a domain where cyber threats and data flows transcend national boundaries.

The study concludes that the effective regulation of AI and ML in cybersecurity requires a balanced approach—one that promotes technological innovation while safeguarding constitutional values, individual rights, and national security interests. Cyber law must evolve from a reactive framework to a proactive governance mechanism capable of addressing emerging technological risks. By strengthening accountability structures, enhancing data protection safeguards, and fostering international cooperation, legal systems can better keep pace with rapid advancements in AI and ML. Ultimately, a forward-looking and principled regulatory approach is essential to ensure that AI-driven cybersecurity serves as a tool for protection rather than a source of legal and ethical vulnerability.