AI and Cybercrime: A Comparative Analysis of Indian, EU, and US Regulatory Models

Prashant Kumar Chauhan, Ph.D., Faculty of Law, University of Lucknow.

Abstract

Artificial Intelligence (AI) has emerged as both a potent instrument and a vulnerable target in the ever-evolving landscape of cybercrime. Its deployment ranges from enhancing cybersecurity infrastructure and predictive policing to facilitating sophisticated cyberattacks, such as deepfakes, autonomous phishing bots, AI-generated ransomware, and algorithmic manipulation. Simultaneously, AI systems themselves are increasingly being targeted by adversaries through techniques like data poisoning and adversarial attacks, exposing critical vulnerabilities. The legal and regulatory frameworks to govern such dual-use technology, however, remain fragmented and underdeveloped across jurisdictions.

This paper undertakes a comparative legal analysis of the regulatory approaches to AI and cybercrime adopted by India, the European Union, and the United States. It identifies the key strengths and shortcomings of each model, examining the extent to which existing legal instruments address the attribution of liability, automated decision-making, and protection of digital rights in the context of AI-driven cyber threats. While the European Union moves towards a unified and risk-based approach through the proposed AI Act, the United States adopts a sectoral, innovation-driven model, and India grapples with regulatory vacuum amid fast-paced digital transformation.

The paper aims to contribute to the discourse on harmonising AI governance with cybercrime control and proposes strategic legal reforms in India by drawing insights from global best practices and institutional experiences.

Keywords*: Artificial Intelligence (AI), Cybercrime, Cybersecurity Infrastructure, European Union, United States, AI-Driven Cyber Threats.*

1. Introduction:

The digital age has witnessed an unprecedented integration of Artificial Intelligence (AI) across sectors, reshaping the contours of economies, governance, and social interaction. While AI brings enormous potential for innovation and productivity, it simultaneously opens new frontiers for cybercriminal activity. AI has emerged not only as a facilitator of cybercrime through tools such as deepfakes, autonomous malware, and algorithmic phishing but also as its potential victim, particularly in cases of data poisoning and adversarial attacks on learning systems. This dual role complicates the legal and regulatory response, creating a dynamic and rapidly evolving cyber threat landscape.

Cybercrime, traditionally associated with acts such as hacking, identity theft, and the dissemination of malicious code, now manifests in more sophisticated forms due to the capabilities of AI. These include the automated generation of polymorphic code that evades traditional detection systems, targeted misinformation campaigns powered by natural language processing, and real-time behavioural profiling to breach systems with human-like precision. Moreover, the opacity and autonomy of many AI systems introduce profound difficulties in attributing criminal liability, thereby testing the limits of existing jurisprudence on mens rea, actus reus, and vicarious responsibility.[1]

The regulatory response to this phenomenon varies significantly across jurisdictions. In India, despite its aspirations to become a global digital powerhouse, the legal framework for AI remains nascent and fragmented. The Information Technology Act, 2000, while central to cyber regulation, is ill-equipped to address the complexities of autonomous and intelligent systems. The Data Protection regime, which would otherwise form a critical pillar in AI governance, is still evolving through the enactment of the Digital Personal Data Protection Act, 2023.[2] Meanwhile, the European Union (EU) has taken a more proactive and structured stance, most notably through the General Data Protection Regulation (GDPR) and the proposed Artificial Intelligence Act, which together aim to balance innovation with the protection of

[1] Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) 103 *California Law Review* 513, 530–531.
[2] Information Technology Act 2000, and Digital Personal Data Protection Act 2023 (India), No. 22 of 2023.

fundamental rights.[3] The United States, in contrast, follows a sectoral and decentralised approach, relying on a mix of agency guidelines, presidential orders, and industry self-regulation.[4]

Statement of the Problem:

Despite the growing integration of Artificial Intelligence in both cybercrime and cybersecurity, existing legal frameworks in India, the EU, and the US remain fragmented and inadequately equipped to address the complex challenges of attribution, liability, and rights protection in AI-driven cyber offences, necessitating a comparative analysis to inform coherent and future-ready regulatory reforms.

Objectives of the Study:

i. To explore the dual role of AI as both a tool and target in cybercrime.
ii. To analyze and compare the regulatory frameworks of India, the EU, and the US.
iii. To assess attribution and liability issues in AI-assisted cyber offences.
iv. To evaluate institutional and legal responses to AI-driven cyber threats.
v. To recommend reforms for India based on global best practices.

Literature Review:

The emerging field of AI and cybercrime has been examined through multiple disciplinary lenses, with a growing emphasis on legal regulation, rights protections, and transnational governance.

In the European context, **Sandra Wachter, Brent Mittelstadt, and Luciano Floridi** argue in *"Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation"* that Article 22 GDPR offers limited protection against opaque

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [2016] OJ L119/1 (General Data Protection Regulation); Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final.
[4] White House, 'Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People' (October 2022) https://www.whitehouse.gov/ostp/ai-bill-of-rights/ accessed 6 July 2025; Federal Trade Commission, 'Business Blog: Using AI? Hold Yourself Accountable or Be Ready for the FTC to Do It for You' (25 April 2021) https://www.ftc.gov accessed 6 July 2025.

AI decision-making[5]. Their critique informs ongoing debates on the EU AI Act, where **Edwards and Veale** (2021) highlight the act's potential for bureaucratic overreach in *"Slave to the Algorithm? Why a Right to Explanation is Probably Not the Remedy You Are Looking For"*[6].

In the US, **Ryan Calo**'s seminal article *"Robots and Privacy"* (2011) frames the privacy risks of embodied AI systems, while **Danielle Citron and Frank Pasquale** (2014) in *"The Scored Society"* emphasize the discriminatory impact of algorithmic profiling[7]. **Woodrow Hartzog** adds to this discourse by critiquing the FTC's fragmented approach to AI regulation in *"Privacy's Blueprint"* (2018), advocating for a unified AI governance framework[8].

Indian scholarship, though nascent, is increasingly critical. **Apar Gupta** has written extensively on surveillance and algorithmic accountability in India, particularly in his essays for the Internet Freedom Foundation[9]. **Ujwala Raje** in her article *"Artificial Intelligence and the Indian Legal System"* (2020) argues that the IT Act, 2000 is outdated and lacks provisions for AI-specific offences[10]. Policy contributions from **NITI Aayog's National Strategy for AI (2018)[11]** and **Vidhi Centre's 2021 report on Algorithmic Governance[12]** further highlight the need for a harmonised legal and institutional response.

Collectively, these works form the theoretical and regulatory basis for evaluating India's position relative to the more developed regimes in the EU and US.

---

[5] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76.
[6] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to an Explanation is Probably Not the Remedy You Are Looking For' (2021) 16 *Duke Law and Technology Review* 18.
[7] Danielle Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1; Ryan Calo, 'Robots and Privacy' in Patrick Lin, Keith Abney and George A Bekey (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press 2011) 187.
[8] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018).
[9] Apar Gupta, 'India's Surveillance Reform Must Begin with a Robust Data Protection Law' (Internet Freedom Foundation, 23 July 2021) https://internetfreedom.in/indias-surveillance-reform/ accessed 7 July 2025.
[10] Ujwala Raje, 'Artificial Intelligence and the Indian Legal System: Challenges and the Way Forward' (2020) 6 *Journal of Indian Law and Society* 112.
[11] NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (Government of India, 2018) https://niti.gov.in/national-strategy-artificial-intelligence accessed 7 July 2025.
[12] Vidhi Centre for Legal Policy, *Algorithmic Governance: The Future of Decision-Making in India* (2021) https://vidhilegalpolicy.in/research/algorithmic-governance/ accessed 9 July 2025.

Research Questions:

This article undertakes a comparative legal analysis of the AI–cybercrime nexus through the lens of three jurisdictions: India, the European Union, and the United States. It seeks to address the following research questions:

- How is AI implicated in contemporary cybercrime, both as a tool and a target?
- What are the legal and institutional mechanisms in place in India, the EU, and the US to regulate AI-driven cyber threats?
- What comparative insights can be drawn to enhance India's regulatory framework?

Methodology:

The methodology employed is doctrinal and comparative in nature, drawing upon statutes, judicial precedents, policy documents, and international conventions. The focus remains primarily on public law instruments and enforcement models, with attention also given to institutional design and due process safeguards.

Paper Structure:

This paper is structured as follows:

Section 2 outlines the conceptual framework linking AI and cybercrime.
Section 3 analyses India's legal and institutional framework.
Section 4 and **Section 5** examine the EU and US models respectively.
Section 6 provides a comparative evaluation of these frameworks.
Section 7 proposes reforms and strategies for India, and
Section 8 concludes with key findings..

2. Conceptual Understanding of AI and Cybercrime:

Artificial Intelligence (AI), broadly understood as the simulation of human intelligence by machines particularly through processes such as learning, reasoning, and self-correction has witnessed rapid growth in its application across critical digital infrastructures[13]. The term

[13] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449, 2019) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 accessed 9 July 2025.

encompasses a wide range of technologies including machine learning (ML), natural language processing (NLP), neural networks, and computer vision. These systems can process vast amounts of data, recognise patterns, and make decisions with minimal or no human intervention. While such capabilities are transforming industries and public services, they are also increasingly exploited in the domain of cybercrime, thereby expanding both the scale and sophistication of digital threats[14].

Cybercrime, traditionally classified under offences such as unauthorised access (hacking), data breaches, online fraud, and the dissemination of malware, now includes AI-facilitated acts such as deepfake generation, AI-driven phishing (spear phishing), botnet automation, and adversarial attacks on AI systems[15]. The convergence of AI and cybercrime thus demands a nuanced understanding of how these technologies function not only as instruments of crime but also as potential targets and enablers of law enforcement.

(a) AI as a Tool for Cybercriminals

AI technologies are being increasingly weaponised to conduct sophisticated attacks. For instance, ML algorithms can be used to develop polymorphic malware capable of dynamically altering its signature to evade traditional antivirus detection[16]. NLP tools are employed in crafting highly convincing phishing emails or generating fake social media profiles to facilitate identity theft. Deep reinforcement learning is also leveraged in automated vulnerability scanning and exploitation, where systems learn to bypass security measures through trial-and-error simulation[17].

AI-enabled cybercrimes often present a unique challenge to law enforcement agencies due to the scale, anonymity, and automation involved. The use of generative adversarial networks (GANs) for deepfakes or synthetic media has implications for both defamation and election interference, raising constitutional and regulatory concerns[18].

---

[14] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* (Europol 2023) 12–14 https://www.europol.europa.eu/publications accessed 5 July 2025.

[15] UNODC, *The Use of Artificial Intelligence in Digital Policing and Countering Cybercrime* (United Nations 2021) https://www.unodc.org/unodc/en/cybercrime.html accessed 9 July 2025.

[16] Mario Nascimento and others, 'Polymorphic Malware Detection Using Machine Learning Techniques' (2020) 25 *Journal of Computer Virology and Hacking Techniques* 213.

[17] Tomas Mikolov and others, 'Efficient Estimation of Word Representations in Vector Space' (2013) arXiv:1301.3781 https://arxiv.org/abs/1301.3781 accessed 10 July 2025.

[18] Danielle Keats Citron and Robert Chesney, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.

(b) AI as a Target of Cybercrime

Conversely, AI systems themselves are increasingly becoming targets of cyberattacks. 'Data poisoning' a form of attack where malicious data is inserted into the training dataset can corrupt the learning model and lead to unpredictable or biased outputs[19]. Similarly, 'model inversion' attacks can reverse-engineer sensitive information from publicly available AI models. These forms of AI-specific attacks challenge conventional definitions of cybercrime and introduce novel concerns of algorithmic integrity, fairness, and accountability[20].

(c) AI in Crime Detection and Predictive Policing

AI is also used by law enforcement and intelligence agencies to prevent and investigate cybercrimes. Predictive policing tools, facial recognition systems, and behavioural analytics are deployed to forecast criminal activity and track suspects. However, the deployment of such technologies raises fundamental issues related to civil liberties, algorithmic bias, and due process[21].

While AI offers unprecedented efficiency in policing, it also raises ethical and constitutional questions, particularly in jurisdictions where legal safeguards against surveillance are underdeveloped or inconsistently enforced. The use of automated decision-making in criminal justice from risk assessments to sentencing recommendations has already come under intense scrutiny in various jurisdictions, including the United States and the European Union[22].

(d) Attribution and Liability in AI-Assisted Crime

One of the most critical conceptual challenges in this domain is the attribution of legal liability for actions undertaken by autonomous or semi-autonomous AI systems. Traditional doctrines of criminal law, which hinge on human intention (mens rea) and culpable conduct (actus reus), often fall short in assigning responsibility when the AI system operates without direct human

[19] Battista Biggio and Fabio Roli, 'Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning' (2018) 84 *Pattern Recognition* 317.

[20] Nicholas Carlini and others, 'Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks' (2019) arXiv:1902.07064 https://arxiv.org/abs/1902.07064 accessed 10 July 2025.

[21] Rashida Richardson, Jason Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice' (2019) 94 *New York University Law Review* 192.

[22] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41 *Computer Law & Security Review* 105567.

input[23]. Questions also arise regarding whether the developer, operator, or end-user should bear the liability, particularly in cases involving malfunction or misuse of AI systems.

Scholars have debated the possibility of granting 'electronic personality' or sui generis legal status to autonomous systems for purposes of liability attribution a proposition that remains controversial and largely speculative[24]. The absence of clarity on these issues across most legal systems further complicates regulatory efforts.

3. Indian Regulatory Model on AI and Cybercrime:

India's digital landscape is experiencing rapid technological transformation, driven by increased reliance on artificial intelligence (AI), cloud infrastructure, and data-driven governance. However, the legal and regulatory ecosystem has struggled to keep pace with the emerging challenges posed by AI-enabled cybercrime. While India possesses a baseline legal framework through the Information Technology Act, 2000 (IT Act), there remains a conspicuous absence of specific legislative provisions or institutional mechanisms tailored to regulate AI systems or address the liability concerns associated with AI-facilitated cybercrimes[25].

(a) Legal and Policy Framework

The IT Act, 2000 continues to serve as India's primary statute governing digital offences and cybersecurity. While Sections 43 and 66 address unauthorised access and hacking, and Section 66C and 66D deal with identity theft and cheating by impersonation, these provisions were not designed with autonomous, learning-based AI systems in mind[26]. The Act also lacks clarity on how to address crimes committed through or against AI tools, such as deepfakes, autonomous malware, or adversarial attacks on machine learning models.

[23] Samir Chopra and Laurence F White, *A Legal Theory for Autonomous Artificial Agents* (University of Michigan Press 2011).

[24] European Parliament, *Resolution with Recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL), 16 February 2017).

[25] Ministry of Electronics and Information Technology, *Report of the Artificial Intelligence Committee* (Government of India 2018) https://www.meity.gov.in/writereaddata/files/Committtee_on_Artificial_Intelligence_Report.pdf accessed 11 July 2025.

[26] Information Technology Act 2000, ss 43, 66, 66C, 66D.

The **Digital Personal Data Protection Act, 2023 (DPDPA)** represents a significant step toward regulating data processing, which forms the backbone of AI development. However, the Act is data-centric and does not extend to algorithmic accountability, AI risk classification, or AI-specific civil/criminal liability[27]. Moreover, AI governance policies such as the **National Strategy for Artificial Intelligence** released by NITI Aayog in 2018 and the draft **National Data Governance Framework Policy (2022)** are largely advisory and aspirational, lacking statutory backing[28].

Cybersecurity enforcement is currently distributed among multiple authorities, including the **Indian Computer Emergency Response Team (CERT-IN), National Critical Information Infrastructure Protection Centre (NCIIPC)**, and various state-level cybercrime cells. CERT-IN's directions issued in 2022 attempt to strengthen incident reporting requirements and digital traceability, but again, these lack explicit reference to AI systems and are criticised for imposing burdensome compliance requirements on digital intermediaries[29].

(b) Judicial Trends and Interpretations

Indian jurisprudence on AI remains in its infancy, with courts yet to directly adjudicate liability in the context of AI-generated or AI-facilitated cybercrimes. Nonetheless, certain constitutional and procedural precedents provide indirect guidance. In ***K.S. Puttaswamy v Union of India***, the Supreme Court held that the right to privacy is a fundamental right under Article 21 of the Constitution[30]. This judgment laid the groundwork for future AI-related privacy and surveillance disputes, particularly concerning facial recognition, biometric tracking, and automated decision-making.

Further, in ***Justice K.S. Puttaswamy (Retd.) v Union of India*** (Aadhaar judgment), the Supreme Court emphasised proportionality and necessity in digital surveillance and data collection, which can be extrapolated to critique state use of AI-powered policing

[27] The Digital Personal Data Protection Act 2023, No 22 of 2023.
[28] NITI Aayog, *National Strategy for Artificial Intelligence* (2018) https://www.niti.gov.in/sites/default/files/2021-09/NationalStrategy-for-AI-Discussion-Paper.pdf accessed 11 July 2025;
Ministry of Electronics and Information Technology, *Draft National Data Governance Framework Policy* (2022) https://www.meity.gov.in/content/national-data-governance-framework-policy accessed 11 July 2025.
[29] CERT-IN, *Directions under Section 70B of the IT Act 2000 relating to Information Security Practices* (28 April 2022) https://www.cert-in.org.in accessed 11 July 2025.
[30] KS Puttaswamy v Union of India (2017) 10 SCC 1.

technologies[31]. The judiciary has also acknowledged the need for legislative oversight of emerging technologies, but has refrained from prescribing specific regulatory models for AI.

Although lower courts and High Courts have occasionally dealt with cases involving digital impersonation, bot-generated spam, and fake social media accounts, these decisions have primarily invoked the IT Act's generic provisions without engaging with the AI dimensions of such offences[32].

(c) Gaps and Challenges

A major gap in India's regulatory approach lies in the **absence of an AI-specific legal framework**. The current laws do not provide for risk-based classification of AI systems, mandatory human oversight in high-risk applications, or accountability mechanisms for harm caused by autonomous systems. Consequently, attribution of liability whether to the programmer, operator, or end-user remains ambiguous, especially in cases involving AI acting without human intervention[33].

Additionally, **algorithmic bias and discrimination** in AI used for digital policing or surveillance raise serious constitutional concerns under Articles 14 and 21. Without transparent audit mechanisms or legislative checks, the unchecked deployment of such systems may infringe on civil liberties[34].

India's law enforcement agencies also face **capacity constraints**, lacking sufficient expertise in AI forensics, algorithm auditing, and real-time incident response. Cybercrime units at the state level often remain under-resourced and overburdened, making them ill-equipped to investigate AI-generated threats such as automated ransomware or deepfake-based extortion[35].

Finally, the **fragmented nature of governance** with overlapping mandates of CERT-IN, NCIIPC, and state cyber cells results in jurisdictional uncertainty and weak coordination in responding to AI-driven cyber incidents[36].

---

[31] Justice KS Puttaswamy (Retd) v Union of India (2019) 1 SCC 1 (Aadhaar case).
[32] Pavan Duggal, *Cyberlaw: The Indian Perspective* (3rd edn, Saakshar Law Publications 2023) 86–90.
[33] Shashank Mohan and Chinmayi Arun, 'Artificial Intelligence and the Law in India' (2019) 14(2) Indian Journal of Law and Technology 1.
[34] Usha Ramanathan, 'Surveillance and the Right to Privacy in India' (2019) 5(1) NUJS L Rev 1.
[35] Rajnish Sharma, *Cybercrime Investigation in India: Challenges and Legal Framework* (Universal Law Publishing 2022) 122–124.
[36] Abhinav Mishra, 'The Need for a Unified Cybersecurity Framework in India' (2021) 2(4) Journal of Law and Policy Review 45.

4. European Union Model: GDPR and AI Act

The European Union (EU) has emerged as a global frontrunner in the regulation of both artificial intelligence (AI) and cybersecurity. Its approach is characterised by strong normative commitments to fundamental rights, transparency, and accountability. Unlike India's reactive and fragmented regulatory stance, the EU has proactively sought to harmonise the governance of emerging technologies through a robust legal framework. Central to this endeavour are the **General Data Protection Regulation (GDPR)** and the **proposed Artificial Intelligence Act (AI Act)**, which together form a layered and risk-sensitive model to regulate AI, data use, and associated cyber threats[37].

(a) Key Legal Instruments

The **GDPR**, enforced since May 2018, is the cornerstone of EU data protection law. It applies to all entities processing personal data of EU residents, regardless of the location of the data controller or processor. Article 22 of the GDPR provides individuals the right **not to be subject to a decision based solely on automated processing**, including profiling, which significantly affects them[38]. This provision is central to the regulation of AI-driven systems, especially in contexts such as algorithmic sentencing, biometric surveillance, and credit scoring.

Additionally, the **AI Act**, proposed by the European Commission in April 2021 and provisionally agreed upon in 2024, is the **first-ever legal framework exclusively addressing AI**. It adopts a **risk-based classification model**, distinguishing between unacceptable, high-risk, limited-risk, and minimal-risk AI systems. High-risk systems such as those used in law enforcement, critical infrastructure, or biometric identification are subject to stringent compliance obligations, including human oversight, data governance, and conformity assessments[39].

---

[37] European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

[38] GDPR, art 22; see also Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76.

[39] European Commission, *Artificial Intelligence Act Proposal*, COM(2021) 206 final, Title II (Risk Classification), Title III (High-Risk AI Systems); see also European Parliament and Council, *Compromise Text on the AI Act* (2024, provisionally agreed).

In the realm of cybersecurity, the **Cybersecurity Act (Regulation (EU) 2019/881)** empowers the **European Union Agency for Cybersecurity (ENISA)** and establishes a certification framework for ICT products and services. While not AI-specific, this act complements the GDPR and AI Act by addressing the **technical resilience of digital systems**, including those embedded with AI components[40].

(b) Institutional Mechanisms

The implementation of AI and cybersecurity regulation in the EU is supported by a **network of institutions**, including:

i. The **European Data Protection Board (EDPB)**, which issues guidance on the interpretation of GDPR in relation to AI.
ii. The proposed **AI Office**, responsible for coordinating the enforcement of the AI Act and maintaining a public database of high-risk AI systems.
iii. **National Supervisory Authorities**, tasked with monitoring AI deployments and ensuring regulatory compliance.
iv. **ENISA**, which conducts threat intelligence, cybersecurity capacity building, and certification under the Cybersecurity Act[41].

These institutional arrangements reflect the EU's emphasis on **preventive regulation** and multi-level enforcement. Notably, the EU mandates **pre-market conformity assessments** for high-risk AI systems and encourages cross-border collaboration through the European Cybercrime Centre (EC3) under Europol[42].

(c) Strengths and Weaknesses

The EU's regulatory model exhibits several **normative and procedural strengths**:

i. **Comprehensive coverage** of AI risks, including direct provisions on data protection, transparency, and accountability.
ii. **Human-in-the-loop safeguards** in high-risk AI contexts, ensuring that critical decisions affecting individual rights are not made solely by machines.

---

[40] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act) [2019] OJ L151/15.

[41] European Data Protection Board (EDPB), *Guidelines 05/2021 on the Interplay Between the Application of Article 3 of the GDPR and the Provisions on International Transfers as per Chapter V of the GDPR* (adopted 18 November 2021); see also European Commission, 'Questions and Answers: The New Artificial Intelligence Office' (2024).

[42] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* (Europol, 2023) https://www.europol.europa.eu/publications-events accessed 12 July 2025.

iii. **Horizontal applicability** of the GDPR and AI Act across sectors and jurisdictions, with extraterritorial scope.

However, the model is not without criticism. Scholars and industry bodies have raised concerns that the AI Act may lead to **regulatory overreach**, resulting in **innovation chill** and **compliance burdens**, especially for startups and small enterprises[43]. Moreover, the delineation between high-risk and limited-risk systems is not always clear, which could give rise to **legal uncertainty** and **administrative complexity**.

The GDPR's broad interpretation of automated decision-making has also faced enforcement inconsistencies across member states, with some data protection authorities adopting restrictive views on what constitutes "solely automated" processing[44]. Additionally, **criminal liability frameworks** for AI-related cybercrimes remain largely underdeveloped, with existing directives such as the **Cybercrime Directive (2013/40/EU)** needing further alignment with AI-specific threats[45].

5. United States Approach: Sectoral and Decentralised Regulation

The regulatory landscape governing artificial intelligence and cybercrime in the United States is marked by **sectoral specificity**, **state-federal fragmentation**, and a preference for **innovation-friendly oversight**. Unlike the European Union's rights-centric and risk-based model, the United States has adopted a **technology-neutral, industry-led approach** that emphasises guidelines, voluntary compliance frameworks, and agency enforcement over comprehensive statutory regulation. While this facilitates rapid AI development, it has also generated gaps in accountability, enforcement inconsistency, and challenges in addressing AI-specific cybercrime[46].

[43] European Digital SME Alliance, *Position Paper on the EU Artificial Intelligence Act* (2022); European Parliament Research Service, *The AI Act: Risks, Impacts and European Values* (2023) PE 698.792.

[44] Christopher Docksey, 'Automated Decision-Making Under the GDPR: A Right to Explanation?' in Gloria González Fuster and others (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar 2020) 253.

[45] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8; Theodore Christakis, 'AI and EU Criminal Law: How to Tackle Artificial Intelligence in Future Cybercrime Reforms' (2023) 9 *European Criminal Law Review* 101.

[46] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2018) 51(2) UC Davis L Rev 399.

(a) Regulatory Framework

The United States does not have a single, overarching federal law governing AI or cybercrime. Instead, its framework is a patchwork of older computer crime statutes, sector-specific data laws, and administrative regulations:

i. The **Computer Fraud and Abuse Act (CFAA), 1986** criminalises unauthorised access to protected computers, and is often invoked in prosecuting hacking, data breaches, and cyber-espionage. However, it does not account for AI as either an offender or a subject of crime, nor does it define liability for autonomous systems.[47]

ii. The **Electronic Communications Privacy Act (ECPA), 1986**, addresses interception of digital communications, but lacks provisions for AI-mediated surveillance, botnets, or algorithmic eavesdropping.

iii. The **AI Bill of Rights (2022)** a non-binding policy document released by the White House Office of Science and Technology Policy proposes five key principles for ethical AI use: safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and human alternatives[48].

iv. In 2023, the **Executive Order on Safe, Secure, and Trustworthy AI** further directed federal agencies to develop sector-specific guidance and testing protocols for high-risk AI systems[49].

v. The **NIST AI Risk Management Framework (2023)**, developed by the National Institute of Standards and Technology, provides voluntary technical and ethical benchmarks for the development and deployment of AI, including guidance on adversarial robustness and system security[50].

Although these instruments signal a growing regulatory focus on AI, none of them create binding criminal liability frameworks for AI-driven cyber offences, leaving enforcement to traditional cybercrime laws.

---

[47] Orin S Kerr, 'Norms of Computer Trespass' (2003) 116 Harv L Rev 1143; Computer Fraud and Abuse Act 18 USC § 1030.

[48] The White House Office of Science and Technology Policy, 'Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People' (October 2022) https://www.whitehouse.gov/ostp/ai-bill-of-rights/ accessed 6 July 2025.

[49] Executive Order No 14110, 'Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence' (30 October 2023) 88 Fed Reg 75191.

[50] National Institute of Standards and Technology, 'Artificial Intelligence Risk Management Framework 1.0' (January 2023) https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf accessed 12 July 2025.

(b) Institutional Oversight

The decentralised nature of the American legal system has led to the proliferation of federal, state, and agency-specific institutions addressing AI and cyber threats:

i. The **Federal Trade Commission (FTC)** plays a pivotal role in regulating deceptive AI practices, particularly under the **unfair and deceptive trade practices (UDTP)** clause of the Federal Trade Commission Act. The FTC has issued multiple warning letters and enforcement actions against entities using biased or opaque algorithms in consumer-facing applications[51].

ii. The **Department of Justice (DOJ)** and the **Federal Bureau of Investigation (FBI)** are responsible for investigating cyber offences under the CFAA and other federal statutes. The **Cybersecurity and Infrastructure Security Agency (CISA)** provides national-level cybersecurity readiness and support.

iii. States such as California, Illinois, and New York have enacted their own statutes to regulate algorithmic transparency, biometric data use, and data breach notification, leading to **regulatory diversity across jurisdictions**[52].

The **absence of a federal AI regulator** or uniform liability framework has led to enforcement inconsistencies, especially in civil rights, consumer protection, and criminal attribution domains.

(c) Critical Evaluation

The U.S. model has several identifiable strengths:

i. It is **flexible and innovation-oriented**, avoiding overregulation and enabling technological competitiveness.

ii. Agencies like the FTC and NIST offer **targeted, evolving guidance** in response to real-world use cases.

iii. The **plurality of state-level initiatives** fosters experimentation and responsiveness to local needs.

However, the model also exhibits critical weaknesses:

[51] Federal Trade Commission, 'Aiming for Truth, Fairness, and Equity in Your Company's Use of AI' (April 2021) https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai accessed 12 July 2025.

[52] California Consumer Privacy Act 2018 (Cal Civ Code §§ 1798.100 – 1798.199); Illinois Biometric Information Privacy Act 2008 (740 ILCS 14); New York Stop Hacks and Improve Electronic Data Security Act 2019 (SHIELD Act).

i. **Fragmentation and inconsistency** in enforcement make it difficult to ensure predictable legal outcomes for AI-related harm[53].
ii. **Lack of statutory clarity** on AI accountability or risk classification means that AI-generated cybercrimes are prosecuted under laws not designed for autonomous behaviour.
iii. There is **no mandatory risk assessment, human oversight, or transparency requirement** across most AI deployments, except when imposed by individual agencies or litigation.

Furthermore, **civil liberties concerns** have surfaced with the use of facial recognition technologies by law enforcement, often disproportionately affecting minorities. The absence of comprehensive federal AI regulation exacerbates concerns regarding algorithmic bias, surveillance, and digital discrimination[54].

6. Comparative Analysis of India, EU, and US:

The preceding sections have demonstrated that while India, the European Union (EU), and the United States (US) all recognize the legal and ethical complexities of artificial intelligence in the context of cybercrime, their regulatory responses reflect distinct priorities, capabilities, and normative foundations. This section presents a comparative evaluation of their frameworks across multiple parameters, including **legal scope**, **institutional strength**, **regulatory coherence**, and **rights protections**.

(a) Regulatory Philosophy and Legal Design

The **EU's approach** is preventive and principled, grounded in fundamental rights and human dignity, as reflected in the **GDPR** and the **AI Act**. It adopts a **risk-based classification model**, legally mandating **transparency, human oversight, and accountability** for high-risk AI systems. In contrast, the **US follows a sectoral and innovation-driven model**, where AI regulation is shaped by agency guidelines and state-level initiatives. While this allows for rapid deployment of AI, it lacks uniform accountability standards and creates **fragmented enforcement**.

[53] Woodrow Hartzog and Evan Selinger, 'The Dangers of Surveillance' (2018) 61(1) Comm ACM 34.
[54] American Civil Liberties Union (ACLU), 'The Case Against Face Recognition Technologies' (May 2020) https://www.aclu.org/report/case-against-face-recognition-technologies accessed 12 July 2025.

India, meanwhile, has yet to articulate a comprehensive AI governance regime. Its reliance on the **IT Act, 2000** and newly enacted **DPDP Act, 2023** does not adequately address AI-specific cyber risks. Regulatory interventions remain policy-oriented and non-binding, as seen in the **National Strategy for AI** and draft frameworks[55].

(b) AI-Specific Cybercrime Liability and Enforcement

The **EU** provides the clearest articulation of algorithmic accountability, including rights against automated decisions (Art. 22 GDPR) and penalties for non-compliant AI systems under the AI Act. It mandates pre-market assessments and post-deployment monitoring, thereby establishing a **proactive liability regime**[56].

In the **US**, enforcement is largely post-facto and focused on deception or harm. The **FTC** acts against unfair trade practices but does not impose technical standards for AI security or criminal accountability. The **CFAA**, while foundational for cybercrime enforcement, is insufficient for autonomous system threats[57].

India lacks any statutory provision that directly addresses **AI-generated or AI-assisted criminal conduct**. Law enforcement agencies rely on general provisions of the IT Act and penal statutes, without clarity on attribution in AI-led attacks or autonomous harms[58].

(c) Institutional Architecture and Capacity

The **EU's layered oversight structure**, involving the **EDPB, AI Office, ENISA**, and national supervisory authorities, reflects a high level of institutional maturity. These bodies are empowered to issue binding decisions, conduct audits, and impose sanctions.

The **US model** is decentralised but functionally robust. Federal bodies like the **FTC, NIST, CISA, and DOJ** play a key role, complemented by state regulators. However, overlaps and jurisdictional inconsistencies persist.

---

[55] NITI Aayog, 'National Strategy for Artificial Intelligence' (2018); Ministry of Electronics and Information Technology, 'Draft National Data Governance Framework Policy' (May 2022) <https://www.meity.gov.in> accessed 12 July 2025.
[56] European Commission, 'Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM(2021) 206 final.
[57] Computer Fraud and Abuse Act 1986, 18 USC § 1030.
[58] Ujwala Hegde, 'Artificial Intelligence and Criminal Liability in India: Issues and Challenges' (2022) 8(1) NUJS L Rev 123.

India's institutional framework is **fragmented and under-resourced**. Bodies like **CERT-IN and NCIIPC** operate with limited AI expertise, and state-level cybercrime cells face technical and manpower shortages. There is no dedicated national AI regulator or AI testing/certification authority[59].

(d) Rights and Due Process Protections

The EU remains the **global benchmark** for AI-related civil liberties. Its legal architecture emphasises **informed consent, human control, data minimisation**, and redressal mechanisms. The **right not to be subject to solely automated decisions** and obligations for **explainability** underscore the primacy of digital human rights.

The US, despite constitutional safeguards like the **Fourth Amendment**, lacks strong federal data protection laws or algorithmic transparency mandates. Concerns over **surveillance, algorithmic bias**, and **facial recognition abuses** have prompted advocacy for a federal AI accountability act[60].

India's digital rights regime is **constitutionally founded but poorly operationalised**. The **Puttaswamy judgment** guarantees privacy, but implementation gaps remain. Predictive policing and biometric surveillance tools are often deployed without judicial or legislative oversight, raising serious due process concerns.

[59] NASSCOM, 'AI Adoption and Regulation in India' (2023) <https://nasscom.in> accessed 6 July 2025.

[60] **Algorithmic Accountability Act of 2023, HR 6580, 118th Congress (US Congress, 2023); American Civil Liberties Union, 'The Dangers of Facial Recognition Technology' (2022) https://www.aclu.org accessed 6 July 2025.**

(e) Tabular Snapshot of Key Contrasts

Feature	European Union	United States	India
Legal Basis for AI Regulation	GDPR, AI Act (proposed)	Sectoral laws, Executive Orders, Guidelines	IT Act 2000, DPDPA 2023 (general only)
Cybercrime Enforcement	Cybercrime Directive, EC3	CFAA, DOJ, FBI, State Laws	IT Act, IPC, State Cyber Cells
Liability Model	Risk-based, proactive, binding	Post-facto, fragmented	Ambiguous, generic provisions
Rights Protections	Strong (Art. 22 GDPR, transparency)	Moderate (FTC, limited privacy laws)	Emerging, privacy judgment only
Institutional Mechanism	EDPB, AI Office, ENISA	FTC, NIST, DOJ, CISA	CERT-IN, NCIIPC, Police Units
Regulatory Approach	Rights-based, preventive	Innovation-oriented, self-regulatory	Policy-based, ad hoc

(f) Lessons for India

The comparative analysis suggests that India may benefit from adopting a **hybrid model** that draws from the EU's normative robustness and the US's innovation facilitation. India urgently requires:

i. A **dedicated AI liability law** with risk-based classifications.
ii. Statutory mandates for **algorithmic transparency, explainability, and human oversight**.
iii. Capacity building of cybercrime units in **AI forensics and digital policing**.
iv. Centralised coordination through a **national AI authority** with enforcement powers.
v. Alignment with **international instruments**, such as the **Budapest Convention** or emerging global AI accords[61].

[61] Council of Europe, 'Second Additional Protocol to the Convention on Cybercrime' (2022); OECD, 'OECD Principles on Artificial Intelligence' (2019) <https://www.oecd.org> accessed 12 July 2025.

7. The Way Forward:

India stands at a crucial juncture where AI innovation and rising cyber threats must be addressed through robust legal and institutional reform. A clear, balanced, and forward-looking strategy is essential to ensure both innovation and accountability in AI governance.

- India should enact a dedicated AI liability law that adopts a risk-based approach similar to the EU AI Act. This law must define AI systems, classify risk levels, and assign liability to developers, operators, or users, with safeguards such as explainability and mandatory impact assessments for high-risk systems.
- The establishment of an independent AI regulatory authority is critical. This body should oversee certification, cross-sector harmonization, and algorithmic audits, while also coordinating with cybercrime units and international agencies.
- Law enforcement capacity must be strengthened through AI forensics training, dedicated cybercrime units, and partnerships with academic and tech sectors for developing tools like deepfake detection and botnet tracking.
- Legal reforms must embed algorithmic transparency and digital rights protections. AI deployment in governance and policing should include human oversight, audit trails, and compliance with Articles 14, 19, and 21 of the Constitution.
- International collaboration is necessary to address cross-border cybercrime and AI misuse. India should align with global frameworks such as the Budapest Convention and GPAI, and enter into MLATs and data-sharing agreements.

Finally, ethical innovation should be incentivised through regulatory sandboxes, certification schemes, and open-source development under strong safety norms.

A hybrid, rights-based, and innovation-friendly framework will enable India to meet the dual challenges of AI governance and cybersecurity while aligning with global standards.

8. Conclusion:

In conclusion, the accelerating convergence of artificial intelligence and cybercrime has redefined the terrain of digital regulation, exposing the limitations of traditional legal frameworks and the urgency of coordinated policy responses. This article has examined how India, the European Union, and the United States have approached the regulatory challenges posed by AI-driven cyber threats, revealing sharp divergences in normative priorities, legal maturity, and institutional design.

The European Union offers a model, and it aims at the fundamental rights and risk-based governance. Using such tools as the GDPR, or the proposed AI Act, it attempts to strike a balance between technological development and algorithmic responsibility or the free will of individuals. The United States, in turn, follows a more industry-specific approach that is innovation-oriented and much relies on agency enforcement, industry standards, and grassroot initiatives. Although this approach promotes the rapid deployment and adaptability that it encourages will be impeded by breakdowns and inequality of protection. Another travesty is that India operates under a feeble and defensive legal system that offers little statutory clarity, institutional rationalization, and accountability systems in an AI-specific context even though it has achieved a lot on digital infrastructure and policy formulation.

A cross-jurisdictional comparison points out that there is no ideal model. Rather, there arises a necessity of a hybrid regulatory system which is flexible, inclusive and embedded in constitutional and human rights principles. In case of India, the future is designing of a customized legal environment, including a risk-based regime of AI regulation, expanding institutional capabilities, protecting internet rights, and participating in international governance arenas in a substantive manner.

The point is, after all, not to control machines, but to control their results. The more autonomy, opacity, and integration AI has with the digital fabric of society, the more the legal system will need to reorganize and develop in order to guarantee that innovation will not come at the expense of security, justice, and democratic control. The law has to be responsive, predictive and above all humanistic.