IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.67

Volume 5, Issue 3, February 2025

Understanding the legal consequences of delayed regulatory regime with respect to Artificial Intelligence

Dr. Pallav Mishra

Student, Late Govindrao Wanjari College of Law, RTM Nagpur University.

Abstract: *The technology related to artificial intelligence can be equated with the discovery of wheel. It only differs from the stated analogy in terms of the state of present nature in which it is conceived, which is highly "civilizational", as opposed to the true 'state of nature' where wheel was discovered. Civilization is founded upon the ideals of limits, controls and moderation; the term intelligence being a natural phenomenon is about to attain artificial characteristics. This blending of natural trait with artificial expression of it – i.e. 'synthesis of intelligence from lifeless vessel', is akin to separating soul from body while body being alive. This is a significant legal problem, for it is touching the essence of civilizational ideals as aforesaid. The presented paper attempts to translate this metaphysical metastasis in legal narrative. The philosophical exposition as explicated above can be understood jurisprudentially through the doctrine of legality – both from domestic and international perspective. For instance, to adjudicate the qualms out of artificial intelligence - specified rules, separate from the conventional ones are to be devised, for - the convectional rules are for natural beings, as opposed to AI regulatory rules, which have no legal acknowledgement and categorization yet. Further, if it is not synchronized in national sphere with due expedience of law, nation as such will face regulatory domination or hegemony at international sphere, resulting due to 'regulatory gap'. The scope of this article consists of possible solutions to the problem at the hand, discussed at length from existing international experiences.*

Keywords: artificial intelligence

I. INTRODUCTION

Artificial intelligence (AI) and emerging technologies present numerous ethical, social, economic, security, and environmental challenges. AI bias and discrimination, deepfakes and misinformation, and privacy violations threaten democratic institutions and personal freedoms, necessitating stricter regulations to prevent mass surveillance and data exploitation. Economically, over-regulation can stifle innovation, while unclear policies discourage investment and create market uncertainty. Countries failing to develop robust AI and semiconductor industries risk global tech dependence on dominant players like the U.S. and Taiwan.[1] From a national security standpoint, AI-driven cybercrime, autonomous warfare, and quantum computing pose significant risks, demanding international regulatory collaboration. Environmental and health concerns also emerge; as unregulated biotech and AI-driven drug discoveries raise ethical questions, and AI's high energy consumption contributes to climate change. Additionally, legal and accountability issues, such as responsibility for AI-caused harm and regulatory fragmentation, complicate compliance for businesses operating across borders. Without a cohesive global approach, the unchecked expansion of AI and emerging technologies could exacerbate social inequalities, economic disparities, and security vulnerabilities worldwide.[2]For an

[1] Georgieva, K. (2024, January 14). *AI will transform the global economy. Let's make sure it benefits humanity*. International Monetary Fund. https://www.imf.org/en/Blogs/Articles/2024/01/14/ai-will-transform-the-global-economy-lets-make-sure-it-benefits-humanity

[2]Qiang, C. Z. (2024, June 27). *What does artificial intelligence mean for the developing world*? World Bank.

instance, if we consider the worldwide interplay between the General Data Protection Regulations (GDPR, 2016) and the newly adopted AI Act (2024), of European Union,which are the most recently available and enforced regulatory regime vis-à-vis AI/ML - it is yet to be understood so as to '*whether they function synergistically to promote responsible AI development or conflict in ways that hinder innovation within the jurisdiction of the union' ?*. While both regulations aim to protect individual rights, their distinct focuses—data privacy under GDPR and AI governance under the AI Act—raise questions about their compatibility. Alegal, ethical, and practical analysis to explore,explicate and simplify the concerning complexities of data protection, algorithmic governance, and ethical AI deployment, needs peremptory legal standing in the form of scaffolding regulations in local context. Such understanding will also contribute to the solution for challenges as such and opportunities at the intersection of data protection and AI governance, thus offset the hurdles for policymakers, and businesses dealing with ever developing AI systems.[3]

Emerging Technologies and their regulation

When countries lack clear regulations for rapidly evolving technologies like AI, blockchain, biotech, and quantum computing, they face several risks and challenges. The legal enforcement of AI within the EU emphasizes both its potential benefits (enhancing crime prevention, investigation, and prosecution) and the legal and ethical challenges it presents, particularly concerning fundamental rights. For instance, the introduction of**ALIGNER Fundamental Rights Impact Assessment**, a tool designed to help law enforcement agencies to assess and ensure that AI deployments comply with fundamental rights and adhere to ethical standards. It explored the tensions between AI in law enforcement and the EU's **Charter of Fundamental Rights** and provided an overview of AI governance developments and best practices, tounderstand how these will be relative to the **Artificial Intelligence Act**; a new regulation aimed at ensuring responsible AI use. Ultimately, all the stress is upon the need for careful AI integration to balance security goals with the protection of individual rights[4].

Emerging concerns and present solution models:

As seen above, artificial intelligence (AI) and emerging technologies present significant ethical and social risks if left unregulated. One major concern is *AI bias and discrimination*, where biased algorithms can reinforce social inequalities in hiring, healthcare, policing, and lending. For instance, AI-driven hiring tools have been found to favour men over women due to training data reflecting historical gender biases. Similarly, AI-powered risk assessment tools in policing have disproportionately flagged minority communities, leading to unfair targeting. Another rising challenge is *deepfakes* and misinformation, where AI-generated fake videos and news can manipulate public opinion and undermine democratic processes. Deepfake political videos have already been used to influence elections, and without legal oversight, the spread of AI-generated misinformation remains unchecked. Additionally, privacy violations and mass surveillance pose a serious threat, as weak data protection laws allow corporations and governments to exploit personal data for monitoring citizens. AI-driven facial recognition in China, for example, has enabled mass surveillance, whereas the EU's General Data Protection Regulation (GDPR) enforces stricter privacy rules to mitigate such risks. Without strong regulations, these technologies can exacerbate discrimination, political instability, and privacy erosion on a global scale.

Beyond social concerns, unregulated AI and tech policies can lead to economic and competitive disadvantages for nations. But on other hand,over-regulation can hinder innovation by making compliance overly burdensome, pushing

https://www.worldbank.org/en/news/podcast/2024/06/27/artificial-intelligence-ai-digital-developing-economies-development-podcast

[3] Butt, J. S. (2024). The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of... *ResearchGate*, *20*(02), 07-52. https://www.researchgate.net/publication/384682777

[4] Casaburo, D., & Marsh, I. (2024). Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: The ALIGNER Fundamental Rights Impact Assessment. *AI Ethics*, *4*(4), 1569–1582. https://doi.org/10.1007/s43681-024-00560-0

startups and companies to relocate to more business-friendly regions. The EU's strict AI laws, for example, may encourage companies to shift operations to the U.S. or Asia, where regulations are more relaxed. Whereas, unclear regulations create market uncertainty and deter investment. The U.S. SEC's vague stance on cryptocurrency, for instance, has caused companies like Coinbase and Binance to focus on regions with clearer regulatory frameworks. Moreover, global tech dependence remains a growing concern, as countries that lack domestic AI and semiconductor industries risk relying on foreign tech giants like Google, OpenAI, and Nvidia. The global semiconductor chip shortage exposed vulnerabilities in India and Europe, as they depend heavily on U.S. and Taiwan-based chip manufacturers. Without strong national AI policies, countries risk falling behind in innovation while increasing dependence on external tech powers.

AI Technologies, Rule of Law and Doctrine of Legality

The rapid advancement of Artificial Intelligence (AI) technologies has raised significant legal and ethical concerns, particularly regarding their alignment with the **Doctrine of Legality**. The principle of legality is fundamental in legal systems that requires laws to be clear, publicly accessible, and not applied retroactively. It ensures that individuals and entities can predict legal consequences and safeguards against arbitrary governance.[5]

Challenges Posed by AI to the Doctrine of Legality[6]

Lack of Transparency ("Black Box" AI) – Many AI systems operate through complex deep learning models, making it difficult to explain how decisions are made. This conflicts with the legal requirement of predictability and accountability.

Bias and Discrimination – AI models trained on biased data may perpetuate discrimination, violating principles of legal fairness and equal treatment.

Retroactivity and Algorithmic Changes – AI models frequently update based on new data, leading to potential retroactive effects where past actions are judged differently under new AI-generated rules.

Liability and Accountability – The **attribution of legal responsibility** in AI-driven decisions remains unclear. Whether responsibility lies with the developer, user, or the AI system itself is still debated in legal circles.

AI technologies, particularly in automated decision-making systems, challenge traditional legal frameworks. AI-powered systems in criminal justice, employment, and finance make decisions that impact fundamental rights, yet their decision-making processes lack transparency. The legal requirement for laws to be clear, foreseeable, and non-retroactive is often difficult to apply to AI, given its reliance on machine learning algorithms that evolve over time, sometimes without direct human oversight.[7]

From a national security perspective, the lack of AI and cyber regulations presents security risks cybersecurity threats and national. The growing capabilities of AI-driven hacking have escalated concerns over **cybercrime**, with incidents like the 2021 Colonial Pipeline cyberattack in the U.S.[8], which disrupted fuel supplies across the East Coast. AI-powered ransomware attacks are becoming more sophisticated, and without updated cyber laws, these threats could proliferate unchecked. Additionally, the weaponization of AI and autonomous warfare poses ethical and legal challenges. Nations are developing autonomous weaponry such as AI-powered loitering drones, which can target and

[5] Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. *University of California Law Review*, *51*(2), 399–419.

[6] Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation." *AI Magazine*, *38*(3), 50–57

[7] Wachter, S., Mittelstadt, B., &Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the Regulation. *International* General Data Protection *Data Privacy Law*, *7*(2), 76–99.

[8] Cybersecurity and Infrastructure Security Agency. (2023, May 7). *The attack on Colonial Pipeline: What we've learned and what we've done over the past two years.* U.S. Department of Homeland Security. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

DOI: 10.48175/IJARSCT-23453

eliminate threats without human intervention, raising concerns about accountability and potential misuse. The absence of international oversight on AI military applications could lead to an AI arms race. Furthermore, quantum computing presents a looming security risk, as its ability to break existing encryption standards could compromise banking, military, and government data security. Without global regulations on quantum security, sensitive information worldwide remains vulnerable to cyber espionage and cyberattacks, putting national security at significant risk.

Finally, emerging AI and tech advancements introduce environmental, health, and legal challenges that demand urgent attention. Unregulated biotech and genetic engineering raise profound ethical dilemmas, particularly in cases like China's 2018 CRISPR-edited babies[9] **scandal**, where gene-editing technology was misused to alter human embryos. While AI-powered drug discovery holds promise, a lack of clear laws could lead to unethical experimentation and unforeseen health risks. Moreover, **AI's carbon footprint** has become an overlooked yet critical concern. Training large-scale AI models, such as **GPT-4**, consumes massive energy, with some estimates suggesting that a single AI model training session emits as much carbon as five cars over their lifetime. Without global standards for sustainable AI development, AI-driven innovations could significantly contribute to climate change. Additionally, legal and accountability challenges emerge as AI becomes more autonomous. *Who bears responsibility when an AI system causes harm?* This question remains unanswered in cases of self-driving car accidents, where liability is unclear—should the developer, the user, or the AI itself be held accountable? Lastly, global regulatory fragmentation creates compliance issues for multinational companies, as different countries enforce conflicting AI and tech laws. For instance, the EU AI Act's strict compliance measures contrast sharply with the U.S.'s decentralized AI regulations, making it difficult for businesses to navigate international markets. Without coordinated global policies, nations and corporations will struggle to maintain ethical and legal consistency in the rapidly evolving AI landscape. Adapting IPR frameworks to the AI era will foster innovation while maintaining fair legal protections. By addressing the legal, ethical, and policy challenges proactively, countries can create an environment where AI-driven advancements thrive without undermining human contributions to innovation.[10]

Contemporarily active approaches to regulation of AI and related technologies

Artificial Intelligence

The European Union follows a strict, risk-based regulatory approach with the EU AI Act (2024), which establishes a framework for AI compliance based on risk levels. In contrast, the United States adopts a decentralized, sector-specific regulation model, with Biden's Executive Order on AI (2023), FTC oversight for AI bias, and various state-level laws shaping AI governance. Meanwhile, India takes a more laissez-faire, case-by-case approach, as it currently lacks a standalone AI law, though AI oversight is proposed under the Digital India Act.

Data Privacy & Protection

The **European Union** has the strongest privacy laws, with the **General Data Protection Regulation (GDPR) (2018)**setting strict data protection rules and imposing significant fines for violations. The **United States,** on the other hand, follows a **fragmented, state-driven approach**, lacking a federal privacy law but with states like **California leading the way through the California Consumer Privacy Act (CCPA).** Meanwhile**, India's privacy framework is new and evolving,** with the **Digital Personal Data Protection (DPDP) Act (2023)** being the country's first digital privacy law. While GDPR remains the most stringent privacy regulation globally, the U.S. relies on state-level initiatives, and India's DPDP Act, though inspired by GDPR, has **weaker enforcement mechanisms**

[9] Ledford,Heidi, (2019). *The AI revolution is coming fast. But are we ready for it?* Nature. https://www.nature.com/articles/d41586-019-01906-z

[10]Nyaboke, Y. (2024). *Intellectual property rights in the era of artificial intelligence.Journal of Modern Law and Policy, 4*(2), 57–72. https://doi.org/10.47941/jmlp.2162

Cybersecurity & National Security

On March 15, 2024, India's Ministry of Electronics and Information Technology (MeitY) issued a revised advisory concerning the deployment of Artificial Intelligence (AI) models, superseding an earlier advisory from March 1, 2024. This revision was prompted by industry feedback and aimed to address concerns regarding the regulation of AI technologies.[11]This revised advisory reflects the government's responsiveness to industry concerns and underscores the importance of balancing innovation in AI with adherence to legal and ethical standards.

The European Union follows a regulated, cooperative approach to cybersecurity, with the NIS2 Directive (2022) mandating strict cybersecurity measures for critical sectors. In contrast, the United States takes a proactive, security-focused approach, led by agencies like CISA (Cybersecurity and Infrastructure Security Agency) and reinforced through Executive Orders on cyber threats. Meanwhile, India’s cybersecurity framework is still developing but remains largely reactive, relying on the National Cybersecurity Policy (2013) and CERT-In mandates for breach reporting. While the EU emphasizes regulatory compliance and international cooperation, the U.S. prioritizes active threat mitigation, and India is working toward stronger cybersecurity policies but currently lags in enforcement and modernization.[12]

Cryptocurrency & Fintech Regulation

The European Union follows a regulated and structured approach to cryptocurrency, with MiCA (Markets in Crypto-Assets, 2023) establishing a unified framework for crypto regulation across the bloc. In contrast, the United States has an unclear, enforcement-driven stance, with the SEC and CFTC regulating crypto on a case-by-case basis, often through lawsuits against major players like Binance and Coinbase. Meanwhile, India takes a cautious approach, discouraging crypto use through a 30% tax on gains, while the RBI remains opposed to private cryptocurrencies. While the EU leads with the most structured regulatory framework, the U.S. relies on legal battles for oversight, and India focuses on high taxation while developing its own Central Bank Digital Currency (CBDC).

Emerging Tech (Quantum Computing, Biotech, Autonomous Vehicles)

The European Union takes a regulated, ethics-focused approach to emerging technologies, with EU Bioethics Laws governing areas like CRISPR and AI-driven genetics, alongside significant quantum computing funding. In contrast, the United States follows a proactive, investment-driven strategy, with the CHIPS Act (2022) boosting quantum technology and NIH guidelines shaping AI applications in medicine. Meanwhile, India is in the early stages of policy development, with the National Quantum Mission (2023) promoting R&D, while biotech regulations remain under review. While the U.S. leads in funding and technological advancements, the EU prioritizes ethical oversight and structured policies, and India is ramping up investment but still lacks detailed regulatory frameworks in biotech and quantum AI.

The *National Strategy for Artificial Intelligence*, developed by NITI Aayog, outlines India's approach to leveraging AI for economic and social growth. The strategy emphasizes **#AIforAll**, a vision aimed at ensuring AI benefits all citizens through inclusive technology leadership. The document highlights India's potential in AI innovation, given its vast data resources, young workforce, and increasing digital adoption.The report proposes establishing Centre of Research Excellence (COREs) and International Centre’s of Transformational AI (ICTAIs) to drive AI research and application. It also suggests initiatives for data governance, skilling, AI-driven startups, and regulatory frameworks to promote AI adoption while ensuring ethical and fair AI deployment.[13]The report proposes establishing Centre of Research Excellence (COREs) and International Centre of Transformational AI (ICTAIs) to drive AI research and application. It

[11] AZB & Partners. (2024, March 15). *MeitY liberalizes AI advisory dated March 1, 2024, following industry concerns and issues revised advisory on March 15, 2024.* AZB & Partners. https://www.azbpartners.com/bank/meity-liberalizes-ai-advisory-dated-march-1-2024-following-industry-concerns-and-issues-revised-advisory-on-march-15-2024/

[12]European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.* Official Journal of the European Union.

[13] NITI Aayog. (2018). *National strategy for artificial intelligence*. Government of India.

also suggests initiatives for data governance, skilling, AI-driven startups, and **regulatory frameworks** to promote AI adoption while ensuring ethical and fair AI deployment.[14]

II. CONCLUSION: THE NEED FOR BALANCED REGULATION

The EU is the most proactive in regulation – it leads in AI, privacy, and crypto laws, setting global standards.

The U.S. takes a decentralized, sector-specific approach, favouring innovation over strict regulation.

India is cautious but evolving, focusing on taxation and gradual tech policy development.

AI presents both opportunities and challenges to legal principles, particularly the Doctrine of Legality. While AI enhances efficiency and decision-making, its lack of transparency, potential for bias, and evolving nature require robust legal frameworks and regulatory mechanisms. Governments must adapt legal doctrines to ensure AI respects fundamental rights, legal clarity, and accountability.

Countries must close regulatory gaps while ensuring they don't stifle innovation.International cooperation is needed for AI, cybersecurity, and biotech laws to prevent global tech monopolies & misuse.Flexible, adaptive policies (like sandbox regulations) can help governments keep up with fast-evolving technologies.

[14] *Ibid.*