ISSN 2581-7124

THE NORTHCAP UNIVERSITY
Formerly ITM University, Gurugram

NCU LAW REVIEW

VOL. 7, ISSUE 1&2 (JANUARY – DECEMBER 2025)
Special Volume on Law and Technology

Articles

ISSN 2581-7124

NCU LAW REVIEW

VOL. 7, ISSUE 1&2 (JANUARY – DECEMBER 2025)

Special Volume on Law and Technology

Tel.: +91-124-2365811 to 13, Ext: 272
Email: nculawreview@ncuindia.edu
Website: www.ncuindia.edu

RNI Reg. No.: HARENG/2018/75464

NCU Law Review, Vol. 7, Issue 1 & 2 (Jan. – Dec. 2025)

ISSN 2581-7124

Date of publication: May 2026

E-mail: nculawreview@ncuindia.edu

Printed at:

Decorpac (I) Pvt. Ltd.
291 D, Sector 6, IMT Manesar
Dist. Gurugram - 122050

Recommended citation: 7(1&2) NCU L. REV. (2025)

Design and Layout by Ms. Krishna Kaveri

NCU LAW REVIEW (ISSN 2581-7124)

Vol. 7, Issue No. 1&2, January – December, 2025

NCU Law Review is a peer-reviewed biannual academic publication of the Centre of Post-Graduate Legal Studies (CPGLS) at the School of Law (SoL), The NorthCap University (NCU), Gurugram (formerly ITM University, Gurgaon). This publication is an endeavour to serve as a forum for the promotion and circulation of views on contemporary legal issues among members of the legal profession, academicians, and students. The Law Review aims to serve legal research centres, policymakers, and government organisations. The views expressed in this publication are those of the authors and not necessarily those of the Editorial Board of the Law Review.

EDITORIAL NOTE

The NCU Law Review, since its birth, has endeavoured to deliver pioneering and unconventional research. This journal is in succession to the previous issues, and like its predecessors, it aims to bring a variety of legal perspectives to the mind of the reader. This special volume of *NCU Law Review* is dedicated to the theme *Law and Technology*, bringing together a curated selection of peer-reviewed articles presented at the International Conference on Law and Technology organized by the School of Law, The NorthCap University, held on November 01, 2025. The volume reflects critical and contemporary discourse on the evolving interface between legal frameworks and technological advancements, addressing key issues such as artificial intelligence, data protection, cybersecurity, and digital governance. Through these scholarly contributions, the issue seeks to foster interdisciplinary engagement and contribute meaningfully to ongoing academic and policy debates in the digital age.

In the article titled "Data Protection and Privacy in Corporate Transactions: Balancing Legal Compliance and Technological Innovation in India," the authors Ms. Saakshi Gupta & Dr. Manish Kumar Yadav examined the evolving landscape of data protection laws in India and their impact on corporate transactions, particularly for multinational entities. The article emphasizes the need to balance regulatory compliance with technological innovation, highlighting key challenges such as cross-border data transfer and consent frameworks, while proposing best practices for effective data governance.

Ms. Ritika Sharma, in the article titled "Artificial Intelligence vis-à-vis Climate Control Regulations", critically explores the dual role of artificial intelligence as both a tool for efficiency and a contributor to environmental concerns. It underscores the urgent need for regulatory frameworks that can manage AI's ecological footprint while ensuring sustainable technological advancement.

In the article titled "Digital Empowerment and Women's Entrepreneurship in Rural Haryana, the authors, Dr. Saumya Sharma & Mrs. Shikha Yadav, highlight how digital technologies, legal frameworks, and social norms collectively shape women's entrepreneurship in rural Haryana. It argues for a gender-sensitive regulatory approach that fosters inclusive digital participation and sustainable empowerment.

The authors, Ms. Somya Tewari & Ms. Swetanka in the article titled "E-Governance Policies: Case study of Rajasthan in the Post-Covid Period", evaluate the effectiveness of Rajasthan's e-governance initiatives post-COVID-19, focusing on accessibility, citizen participation, and service delivery. It seeks to assess whether digital governance mechanisms have successfully enhanced public engagement and administrative efficiency.

Ms. Aastha Gupta, Dr. Neha Jain, and Asha Srivastava, in the article titled "Viral Suicide Games: Online Psychological Manipulation and Legal Gaps", analyze the phenomenon of online suicide challenges as forms of cyber-enabled psychological coercion. The article identifies critical gaps in existing legal frameworks and advocates for integrating psychological insights into law and policy to better protect vulnerable adolescents.

In the article titled "Cybersecurity Awareness and Capacity Building in India: A Grassroots Approach," Ms. Pakhi Kansal stresses the growing mismatch between cybersecurity policies and public awareness in India, particularly in rural areas. It calls for grassroots, inclusive approach to cybersecurity education to build a digitally resilient society.

Mr. Abhijay Singh, in the article titled "Utilizing Blockchain Technology to Strengthen Intellectual Property Ownership in India", explores how blockchain technology can address persistent challenges in intellectual property protection in India. It highlights the potential of decentralised systems to enhance ownership security while also acknowledging regulatory hesitations and practical limitations.

The authors Vedika Khanna and Dr. Ambika Dutta, in the article titled "Digital Dissonance: Adolescents, Free Speech, and Social Media," investigate how adolescents in India navigate identity, self-expression, and legal boundaries on social media. It reveals the tension between authenticity and social validation while highlighting the role of digital platforms in shaping emerging forms of civic engagement.

In the article titled "Artificial Intelligence Revolutionising Justice: Tackling India's Judicial Backlog", Yash Vats and Kirti Rana propose the use of AI as a tool to address delays in India's judicial system. It advocates for a balanced integration of AI in judicial processes, emphasizing efficiency gains while maintaining human oversight, ethical considerations, and data privacy safeguards.

The Editorial Board expresses heartfelt gratitude to the authors for their scholarly contribution. We would further extend our appreciation to Sh. Avdhesh Mishra, Hon'ble Chancellor, NCU, Hon'ble Members of the Governing Body, NCU; Prof. (Dr.) Prem Vrat, Hon'ble Pro-Chancellor, NCU; Prof. (Dr.) Nupur Prakash, Hon'ble Vice-Chancellor, NCU, for their continuous support, guidance, and cooperation in this academic endeavour. We are also thankful to the reviewers, the dedicated staff of the University, and Decorpac (I) Pvt. Ltd.

Editorial Board

NCU LAW REVIEW

MESSAGE FROM THE VICE CHANCELLOR, NCU

Research is a crucial and revered responsibility of the Higher Education Institutes. Not only is it a way of giving back to the community, but it also ensures the opening up of the academic vistas remaining to be explored. Hence, with immense pleasure, I present you with pride and happiness, vol. 7 of NCU Law Review, published under the aegis of the Centre for Post-Graduate Legal Studies (CPGLS) at the School of Law, The NorthCap University.

Our previous volumes were a success, taking within their fold running currents and trends of law. In fact, the volumes through their amplified circulation reached the hands and minds of legal luminaries in the academic circles and the legal profession. The present journal endeavours to carry the legacy of success forward and keep the vibrancy of legal research vigorous. The law review intends to keep the spirit of inquiry and legal reform alive in the minds of avid readers, young and old academicians, advocates, and aspiring lawyers. The articles published in the journal meticulously scrutinise the legal quagmires and fertilize the soil for further thought and action.

I sincerely appeal to all legal scholars to contribute to the future issues of the law review and further the cause of knowledge.

The publishing, editing, and shaping up of the law review would have been impossible without the determined and accurate work of the editorial team. I congratulate the entire team. I acknowledge my thanks and due regards to the contributors of the journal and hope for our long and continued relationship in the future.

Best Wishes and All the Success!

Prof. (Dr.) Nupur Prakash,
Vice Chancellor,
NCU, Gurugram

TABLE OF CONTENTS

DATA PROTECTION AND PRIVACY IN CORPORATE TRANSACTIONS: BALANCING LEGAL COMPLIANCE AND TECHNOLOGICAL INNOVATION IN INDIA

Ms. Saakshi Gupta[*] *& Dr. Manish Kumar Yadav*[**]

ABSTRACT

For Multinational business (MNCs) and transactional Corporation (TNCs) engaged in transaction involving sensitive personal data in the contemporary digital world, data security personal data in the contemporary digital world, data security and privacy are critical concerns. This study explores the intricate relationship between data protection regulations and technological advancement in global commercial transactions, with an emphasis on India. The authors have looked into the laws that control data protection in India, such as the Information Technology Rule of 2011 and the Digital Personal Data Protection Act of 2023. Important ideas and requirements, such as data localization, cross-border data transfer, and consent procedures, are covered to provide a thorough grasp of the legal frameworks. The challenges MNCs and TNCs operating in India face while managing data privacy rules in the commercial transaction area are examined in this article. In order to achieve a balance between technological innovation and regulatory compliance in commercial transactions, the article outlines strategies and best practices for MNCs and TNCs. It concludes with a discussion on technological developments in India, the potential impact of regulatory reforms, industry standards, and international data transfer mechanisms on corporate data protection practices in order to offer insights into the evolving trends and landscape of data privacy and security.

I. REGULATORY LANDSCAPE OF DATA PROTECTION IN INDIA

Strong Data protection laws are necessary to preserve people's right to privacy and foster trust in digital ecosystems as a result of the expanding digitalization of information, which has boosted data collecting and processing. With important legislation and regulations influencing the corporate landscape, India's data protection regulatory environment has changed dramatically over time.

1.1. An Overview of Data Protection Laws in India

The Information Technology (Reasonable Security Practices, Procedure and Sensitive Personal Data or Information) Rules 2011, enacted under the Information Technology Act of 2000, established guidelines for the collection, storage, and processing of sensitive personal data or information (SPDI). These

[*] The author is an Assistant Professor at Asian Law College and may be reached at guptasakshi018@gmail.com.
[**] The Co- author is a Professor at the Fairfield Institute of Management and Technology, School of Law, GGS Indraprastha University, New Delhi, and may be reached at drmanishyadava@gmail.com.

rules encourage firms handling SPDI to take reasonable security measures and obtain consent from data subjects.[1]

1.2. Key Principles and Requirements

a. Data Localization

Data localization is a key component of India's data protection legislation, requiring certain types of data to be kept and processed solely within India's geographical boundaries. This mandate aims to strengthen data sovereignty, eliminate the risks associated with cross-border data transfer, and promote the development of local data storage infrastructure. However, it poses challenges for foreign corporations working in India, impacting their data management and operational planning.[2]

b. Cross-Border Data Transfers

The standards governing trans-border data transmission play an important role in ensuring the consistent movement of information while upholding protection and security requirements. Bodies transporting information outside of India should adhere to approved processes such as standard authoritative declarations and obtaining express consent from information subjects. These guidelines encourage appropriate data sharing practices while reducing the danger of unwanted access or data breaches during transfers.

c. Consent Mechanisms

Acquiring a legal agreement is critical to lawful information processing under India's information assurance requirements. Bodies should ensure that assent is freely provided, explicit, and informed, with the individual retaining the ability to withdraw their given assent. The Digital Personal Data Protection Act of 2023 includes new consent methods, such as explicit consent in certain settings, age-appropriate consent for children, and more individual data control.

1.3. Impact on Corporate Transactions

The regulatory criteria listed above have important consequences for company transactions in India. Businesses involved in mergers, acquisitions, or partnerships must examine data protection compliance as part of the due diligence process. Compliance with data localization and cross-border data transfer regulations is critical in determining the viability and dangers of such transactions. Furthermore, having strong consent processes and data protection standards is

[1] Aggarwal, Raj and James K.Weekly, "Foreign Operations of Third World Multinationals: A Literature Review and Analysis of Indian companies" 17, *The Journal of Developing Areas*, 13-30, (1982).

[2] Iyer, G. Chidambaran, "Indian Multinationals, Foreign Multinationals and Domestic Firms, 12, 3, *Journal of Economic Policy Reform*, 243-247, (2009).

critical for preserving confidence and regulatory compliance throughout the transaction lifetime.

1.4. Challenges and Opportunities

While India's data protection legislation seeks to improve privacy and security standards, they also provide hurdles to enterprises, notably in terms of compliance costs, operational complexities, and legal unpredictability. The changing nature of technology and data processing activities needs ongoing adaptation to legal standards, necessitating proactive strategies and investments in data governance and compliance frameworks.

However, these constraints provide an opportunity for creativity and collaboration. Businesses that prioritize data protection and implement best practices will gain a competitive edge, create consumer trust, and handle regulatory challenges more efficiently. using technologies like encryption, anonymization, and data localization solutions may improve data security and regulatory compliance, creating an atmosphere for data management and digital transformation[3]

As a result, the legislative landscape for data security in India is dynamic and changing, driven by technical breakthroughs, privacy concerns, and worldwide regulatory trends. Businesses must take a proactive approach to this scenario, prioritizing data security, compliance, and appropriate data management practices. As India strengthens its data protection framework, players from all industries must collaborate, innovate, and adhere to privacy and transparency principles in order to create a trustworthy digital ecosystem for long-term growth and innovation.

II. CHALLENGES FACED BY MNCS/TNCS IN ENSURING COMPLIANCE

The difficulties of navigating regulatory frameworks, particularly in the context of corporate transactions, have increased the difficulties faced by multinational corporations (MNCs) and transnational corporations (TNCs) operating in India. Case Studies offer useful Insight into common compliance pitfalls.

2.1. Compliance Challenges Faced by MNCs/TNCs

a. Regulatory Complexity

The Complexity of data privacy regulations, such as the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023, makes it challenging for MNCs and TNCs operating in India to achieve full compliance. Complicating issues include permission procedures, data localization regulations, and cross-border data transfer, which call for careful legal analysis and strategy preparation.

[3] Nagala, Sarla V, "Indian's Story of Success: Promoting the Information Technology Industry, 6(1), *Stanford Journal of International Relations*, (2005).

b. Data Localization and Cross-Border Data Transfers

MNCs and TNCs with global operations face challenges due to data localization requirements, which mandate that specific categories of data be stored and processed within India's boundaries. It is difficult to maintain data security and integrity while balancing local adherence to international data management regulations. Additionally, managing cross-border data flow while creating regulatory frameworks and sufficiency judgment compliance initiatives leads to regulatory ambiguity and compliance gaps.

c. Consent Mechanisms and Individual Rights

Another significant challenge for MNCs and TNCs is obtaining appropriate consent for data processing operations. Strict data governance frameworks and open communication with data subjects are necessary due to the complexity of consent procedures, which include explicit consent requirements, age-appropriate consent for children, and the right to withdraw consent. Ensuring adherence to individual rights, such as data access, correction, and deletion, increases the complexity of data processing operations and necessitates ongoing review and procedure improvement.[4]

2.2. Enforcement Trends and Penalties for Non-Compliance

Significant changes have occurred in India's enforcement of data protection laws, with regulatory bodies closely monitoring compliance initiatives and enforcing fines for rule violations. The Digital Personal Data Protection Act of 2023 established the Data Protection Authority (DPA), which is essential in monitoring compliance difficulties and enforcing data protection regulations. Penalties for non-compliance, including fines, suspension of data processing operations, and harm to market reputation, highlight the significance of effective compliance frameworks for MNCs/ TNCs operating in India.

Case Studies: Common Compliance Pitfalls and Legal Risks

a. Case Study 1: Cross-Border Data Transfer Non-Compliance

The related case laws are as follows:

One of the most notable instances, including cross-border data transfers, is the "Schrems II" case (2020), which incorporates information transfers between the European Union (EU) and the USA. The Court of the European Union (CJEU) rebuffed the EU-USA Protection Safeguard Structure for this case, raising concerns about U.S.A snooping tactics and the absence of a robust security

[4] Rajnish Tiwari, Cornelius Herstatt, (2010) "The Emergence of Indian Multinationals: An Empirical Study of Motives, Current Status, and Trends of Indian Investment in Germany", in Sauvant, K.P., Pradhan, J.P., Chatterjee, A., Harley, B. *et.al.* (eds.), *The Rise of Indian Multinationals* 56 (Palgrave Macmillan, New York, 2009).

mechanism for the privacy of data of EU citizens communicated to the USA. This case showed the need to lay out genuine information protection while moving private information outside the EU.[5]

A prelude to the above case, often referred to as "Schrems I (2015) case," which laid the foundation for the Schrems II verdict. Max Schrems, an Austrian Security Campaigner, challenged the transfer of his information from Facebook Ireland to servers in the USA, referring to Edward Snowden's disclosures concerning the USA's mass shadowing exercises. The CJEU's decision in this case discredited the EU-USA Safe Harbor Structure, underlining the importance of satisfactory information security strategies for global information transfers.[6]

In another case in the year 2018 involving Max Schrems, the court verified Facebook's utilization of standard legally binding statements (SCCs) for moving individual information from the EU to the USA. The CJEU's decision highlighted the significance of evaluating the adequacy of information assurance in the beneficiary nation, especially concerning government surveillance, while depending on SCCs for cross-border information transfers.[7]

While not directly related to GDPR or EU data protection laws, this case, United States v. Microsoft Corp (2018), is significant for its implications on cross-border data access and privacy. The U.S. Supreme Court ruled that U.S. law enforcement authorities cannot compel American companies to disclose data stored on servers outside the United States of America. This decision has implications for data protection and jurisdictional issues in cross-border data transfer scenarios involving U.S.-based companies.[8]

The above cases demonstrate the complicated legal environment of cross-border data transfers, stressing the significance of following important information assurance guidelines, guaranteeing sufficient protections for global information transfers, and addressing concerns connected with government surveillance and information access.

b. Case Study 2: Consent Mechanism Failures

The related case laws are as follows:

In the case of Google LLC, 2020, the French Conseil d'état (Committee of State) looked for direction from the Court of the European Union (CJEU) with respect to the request for the "right to be forgotten" worldwide. While not specifically about consent mechanism failures, it touches on issues of consent on data

[5] *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*, C-311/18, (2020) Judgment of the Court (Grand Chamber).
[6] *Max Schrems v. Data Protection Commissioner*, C-362/14, (2015) Judgment of the Court, Grand Chamber.
[7] *Facebook Ireland Ltd & Schrems*, C-311/18, (2018) Order of the Court, Grand Chamber.
[8] *United States v. Microsoft Corp*., (2018) 584

processing and the extraterritorial reach of data protection laws, highlighting the importance of clear and valid consent mechanisms.[9]

In the Max Schrems case of 2018, the claim, concerning [10] The utilization of standard legally binding provisions (Standard Contractual Clauses -SCCs) for cross-border information transfers. While not solely about consent mechanism failure, it raised questions about the adequacy of consent obtained from users for data processing activities, particularly when transferring data to countries with different privacy standards.

The Google (2013) case[11] in the United States of America concerned Google's acquisition of Wi-Fi information as part of its Street View mapping project. Google was accused of intercepting and collecting private data from unsecured Wi-Fi networks without obtaining proper consent. The case demonstrated the significance of getting express consent for data-collecting operations, particularly those involving sensitive information.

The Federal Trade Commission (2019) case in the USA settled with Facebook different affirmed protection infringements,[12] including misdirecting clients about the degree to which outsider applications could access their information and neglecting to sufficiently inform clients about information sharing practices. This example illustrates the necessity of using transparent and accurate consent processes to guarantee that customers understand how their data is used and shared.

The UK's Information Commissioner's Office (ICO) has conducted several investigations and enforcement actions in response to consent mechanism failure; this is not a specific case. For instance, companies have been penalized for sending marketing emails without the required consent, highlighting the need to comply with assent requirements under information security regulations such as the General Data Protection Regulation (GDPR).

Therefore, MNCs and TNCs have significant challenges when navigating data privacy laws in India, requiring proactive compliance strategies, legal expertise, and technological solutions. Continuous monitoring, risk assessments, and capacity building programs are required due to the complexity of data localization, cross-border data transfers, consent processes, and enforcement trends. The aforementioned case studies emphasize the necessity for businesses to give data protection, accountability, and transparency top priority in their

[9] *Google LLC v. CNIL*, Grand Chamber of the European Court of Justice, (2020).
[10] *Facebook Ireland Ltd & Schrems Case* (2018), Case C-311/18, Order of the Court, Grand Chamber, (2018).
[11] *Google Inc. Street View Electronic Communications Litigation Case*, 794 F. Supp. 2d 1067 (N.D. Cal. 2011)
[12] *Federal Trade Commission v. Facebook, Inc. Case*, 777 F. App'x 968 (9th Cir. 2019)

operations by illuminating the practical effects of non-compliance. In an increasingly digital environment, MNCs and TNCs can reduce legal risks, build stakeholder confidence, and promote a culture of responsible data management by successfully tackling these issues.

III. Impact of Technological Advancements on Data Protection Practices

In today's digital age, technological advances influence how businesses handle and preserve their information. The impact of technological advancements such as big data analytics, cloud computing, and the Internet of Things (IoT) on data protection policies in corporate transactions, particularly worries about confidentiality and illegal access, cannot be underestimated.

3.1. Big Data Analytics

In today's digital world, technical advancements have a huge influence on how businesses manage and protect their data. Big data analytics is altering corporate information management and storage by enabling firms to make data-driven decisions quickly and efficiently. However, this technique raises data protection concerns.[13]

One of the most pressing issues with large-scale data analytics is data security. As companies gather and analyse huge amounts of data, sensitive information must be protected from illegal access and cyber threats. Furthermore, the use of cutting-edge technology such as AI raises concerns regarding the responsiveness and fairness of information processing approaches.

3.2 Cloud Computing

Cloud computing has altered how organizations store, manage, and access data. Its scalability, adaptability, and cost-effectiveness make it a popular choice for businesses of all kinds. However, the growth of cloud computing creates new issues in data protection.

One of the primary worries about cloud computing is data privacy. Organizations that store information in the cloud rely on third-party suppliers to ensure its security. This raises concerns regarding data sovereignty and compliance with legislations like the General Data Protection Regulation (GDPR) and the Central Consumer Privacy Act (CCPA. and the risk of data breaches. Moreover, the shared infrastructure of a cloud environment can make data more vulnerable to cyberattacks.

[13] H.W. Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology*, (Harvard Business Press, 2003).

3.3 Internet of Things (IoT)

The Internet of Things (IoT) is an organization of connected gadgets that gather and exchange information. In commercial interactions, Internet of Things (IoT) gadgets are used to collect real-time data, increase operational efficiency, and improve consumer experiences. However, the growth of IoT devices raises concerns about data protection.[14] One of the essential issues with IoT is information security. Several IoT gadgets need viable security assurances, leaving them defenceless against digital assaults and hacking. Besides, the enormous amount of information generated by IoT gadgets presents worries concerning information storage, handling, and access limitations. Establishments should set up powerful safety nets to shield IoT information from unapproved access and guarantee compliance with privacy protocols.[15]

3.4 Implications for Data Protection and Privacy

The rapid advancement of technology has significant implications for data protection and privacy in corporate transactions. On one hand, growing advancements offer open doors for innovation on the other, they pose challenges that must be addressed to safeguard sensitive information and maintain trust with stakeholders.[16]

3.5 Data Security

Data security is more important than ever due to the growth of data and the use of cutting-edge technology. To protect data from cyber threats, organizations should use security measures including encryption, access limits, and risk location systems. Furthermore, security upgrades and evaluation are essential for tackling ever more complex data security issues.

3.6 Privacy

To prevent unauthorised exposure od sensitive company information, confidentiality must be upheld. Among the technologies that might assist in maintaining the confidentiality of business transactions are encryption, data masking, and secure communication channels. Additionally, companies should teach staff members about appropriate data protection procedures and create clear policies and procedures for handling personal data.

[14] Zhou J, Cap Z, Dong X, Vasilakos AV. "Security and Privacy for Cloud-based IoT: Challenges," 55(1), *IEEE Commun Mag*, (2017).
[15] Liu T, Yuan R, Chang H., "Research on the Internet of Things in the Automotive Industry," *International Conference on Management of E-Commerce and E-Government, Beijing, China*, (2012).
[16] S. E. Gupta and A. Jain, Data Privacy: An Overview and Challenges in the Era of Big Data, 2018, *available at:* https://arxiv.org/abs/1804.08910, (last visited on March 22, 2024).

3.7 Unauthorized Access

Preventing unauthorized access to data is very critical to data security. Access restriction, multi-factor authentication, and identity management technologies, such as biometrics/ iris scans, can help limit entry to just the permitted personnel. To reduce the danger of unauthorized access, firms must also monitor access records, detect suspicious activity, and respond quickly to security issues.

IV. STRATEGIES FOR BALANCING LEGAL COMPLIANCE AND TECHNOLOGICAL INNOVATION

The strategies and best practices for navigating this intersection are data protection regulations and technological advancements in corporate transactions. Additionally, we can ensure vendor compliance and use privacy-enhancing technologies, such as encryption, to mitigate data protection risks. MNCs and TNCs work in a constantly changing environment where legal compliance and technological innovation intersect.

4.1 Strategies for Navigating Data Protection Regulations

MNCs and TNCs face a complicated scenario of information security guidelines, including GDPR, CCPA, and other territorial and industry-specific regulations. To explore these guidelines successfully, establishments can take on a few practices:

a. Privacy Impact Assessments (PIAs): PIAs help organizations recognize and evaluate the privacy risks related to their information handling exercises. By conducting PIAs, companies can identify potential compliance gaps and implement measures to mitigate privacy risks proactively.[17]
b. Implement Information Assurance by Plan and Default: Information security by plan and default includes incorporating protection considerations into the plan and execution of processes, systems, and products. This approach guarantees that information insurance measures are implemented all along, as opposed to being retrofitted later. Key principles include purpose limitation, data minimization, and privacy-enhancing technologies.
c. Ensure Merchant Compliance: MNCs and TNCs frequently collaborate with outside suppliers and service providers that handle personal data processing on their behalf. Verifying that these providers abide by contract requirements and data protection laws is crucial. This entails

[17] Wright, David, and Paul De Hert, "Introduction to Privacy Impact Assessment.'' in David Wright, Paul De Hert, (eds.) *Privacy Impact Assessment* (Springer Dordrecht, 2012).

putting data protection provisions in contracts and using audits and evaluations to keep an eye on vendor compliance.

4.2 Role of Privacy-Enhancing Technologies and Encryption

a. Privacy-Enhancing Technologies (PETs) and encryption assume a vital role in relieving information security risks for MNCs and TNCs. These technologies provide tools and mechanisms to protect data privacy and confidentiality.
   Key strategies include:[18]
b. Use of Anonymization and Pseudonymization: Anonymization and Pseudonymization procedures help anonymize individual information, lessening the risk of information breaches and unapproved access. By anonymizing information, organizations can perform investigations and handling exercises while safeguarding individual privacy.[19]
c. Encryption of Data: Data that has been encrypted is transformed into a secure format that can only be viewed with the right decryption key. Organizations may safeguard data security and avoid unwanted access or interception by encrypting sensitive data while it's in transit or at rest.

4.3 Best Practices for Balancing Legal Compliance and Innovation

It is necessary to employ best practices and preventative measures to achieve a balance between technical innovation and legal compliance:

a. Keep up with Regulatory changes: MNCs and TNCs need to be abreast of evolving regulations on data protection and compliance. This entails keeping an eye on changes in regulation, regularly reviewing compliance, and updating methods and systems in a similar way.
b. Encourage a Culture of Security Compliance: Businesses should encourage compliance across the board. This entails conducting awareness campaigns, teaching employees about data security principles, and integrating privacy concerns into business operations and decision-making.
c. Work together with stakeholders: Working together with authorities, trade associations, and stakeholders is crucial to effectively navigating the complexities of data security and technological innovation. A Collaborative approach to innovation and compliance may be supported by interacting with others, sharing best practices, and participating in industry projects.

[18] S. Fischer, *Hubner, Privacy – Enhancing Technologies (PET)* Course Description (Karlstad University Division for Information, Karlstad, Sweden, 2001).
[19] A. Escudero Pascual, *Privacy in the Next generation Internet* (Royal Institute of Technology, Kista, Sweden, 2001).

Therefore, finding a balance between technical innovation and regulatory compliance is a strategic imperative for MNCs and TNCs operating in today's global economy. By employing strategies including conducting privacy impact assessments, implementing data protection by design and default, ensuring vendor compliance, and utilizing technologies like encryption that improve privacy, organizations may lower data protection risks while fostering innovation. Moreover, maintaining a harmonious balance between legal requirements and business objectives requires working with stakeholders, fostering a culture of privacy and compliance, and staying updated on current legislative and technological developments.

V. Future Trends and Recommendations

With the increasing digitalization of businesses and the growing significance of data-driven decision-making, India is at a critical junction in the rapidly changing landscape of data protection and technological advancements. It is crucial to analyse future trends and developments in data protection regulations and technological innovations, and to offer recommendations for multinational corporations (MNCs) and transactional corporations (TNCs) to proactively address data protection challenges while leveraging technological advancements in corporate transactions. It is also necessary to talk about the possible effects on corporate data protection policies in India of industry standards, international data transfer systems, and governmental reforms.

5.1 Predictions for Future Trends in Data Protection Regulations

a. Enhancing Data Protection Laws: After the Digital Personal Data Protection Act was passed in 2023. India is modernizing its infrastructure for data security. Stricter regulations for the gathering, storing and use of personal data are among the next changes, in keeping with global standards like GDPR.
b. Data Localization: It is now necessary to store and process some types of data in India. Concerns over national security and data sovereignty are the driving forces behind this movement.
c. Prioritizing privacy by design: New legislation may require companies to include privacy issues in their designs from the start.
d. Enhanced Enforcement Mechanism: As data breaches and privacy violations become more common, regulatory agencies may increase fines and penalties for non-compliance.

5.2 Technological Innovations in Data Protection

a. Blockchain Technology: Blockchain is a visible solution for enhancing data procedures because of its secure and transparent data storage and transfer process.

b. AI Solutions: By automating processes, identifying irregularities, and reacting quickly to security concerns, an AI-powered solution may improve data security.
c. Biometric Validation: Biometric technologies, such as fingerprint and face recognition, are becoming more and more popular for enhancing data security, particularly in access control and identity verification systems.

5.3 Recommendations for MNCs/TNCs

a. Prioritize robust data protection measures, including encryption, access limitations, and regular security assessments, for MNCs and TNCs doing business in India.
b. Conduct Privacy Impact Assessment (PIAs): PIAs help firms comply with regulations by identifying and addressing privacy problems connected to data processing activities.
c. Embrace Privacy-Enhancing Technologies: Adopting technologies like encryption, anonymization, and tokenization can help organizations protect sensitive data while enabling lawful data transfers across borders.[20]
d. Collaborate with Regulators and Industry Bodies: Engaged the regulators and industry bodies, who can provide valuable insights into evolving data protection regulations and best practices, allowing MNCs/TNCs to stay ahead of compliance requirements.

[20] Working Group on "Privacy Enhancing Technologies" of the Committee on "Technical and organization aspects of data V. Senicar et al./ Computer Standards & Interfaces, 147-158, (2003).

ARTIFICIAL INTELLIGENCE VIS-À-VIS CLIMATE CONTROL REGULATIONS

Ritika Sharma*

ABSTRACT

Artificial intelligence (AI) has emerged as a transformative 21st-century technology, evolving from science fiction to ubiquitous reality accessible via the internet. Initially designed for complex, data-intensive tasks beyond human capacity, AI now permeates economies, industries, and daily life, reshaping communication, learning, and decision-making. While this reflects technological progress, it raises concerns about dependency, privacy, environmental costs, and regulatory gaps amid profit-driven competition among tech giants.

This article critically examines AI's intersection with climate change, advocating oversight mechanisms to balance its potential benefits against ecological harms and unregulated expansion. Employing qualitative analysis of research papers, public data, expert discussions, and critical observations, it reveals AI's efficiency gains alongside its substantial carbon footprint and the lack of global governance. Ultimately, dynamic AI regulations are essential to harmonize innovation with environmental sustainability—lest unchecked development, as warned by experts, imperil humanity.

In conclusion, dynamic AI governance—encompassing global standards for energy efficiency, transparency mandates, and ethical audits—is vital to align innovation with sustainability. As Stephen Hawking cautioned, unchecked "full artificial intelligence" could imperil humanity. Prioritizing regulation ensures AI serves as a force for good, not existential threat.

I. INTRODUCTION

Since the beginning of the 21st century, technological systems have experienced an exponential rise in terms of their scale and usage throughout the world. Among these advancements, AI is evolving rapidly and has quickly become one of the most significant innovations that is impacting our lives directly or indirectly. The purpose and aim behind creating such artificial intelligence was to ease the tasks that required complex calculations and a lot of manual computing hours of humans. [1] From building this technology with an aim to simplify intricate mathematical and scientific questions, it has been integrated into areas of art and literature as well. While there are numerous perspectives to consider regarding such advancements, this article focuses on the positive developments in AI, which

* The author is LL.B Student, School of Law, The NorthCap University, and can be reached at ritikash15902@gmail.com.

[1] Stuart Clark, "Artificial intelligence could spell end of human race - Stephen Hawking", *The Guardian* (Dec. 12, 2014).

have helped us progress further for the sake of humanity, but also some foreseeable drawbacks, like its impact on the climate, that were overlooked due to the capitalist mindset and the profit-oriented approach of these AI companies. A study shows that massive data centres can use approximately eleven (11) million litres and nineteen (19) million litres of water per day[2], for cooling down their systems that heat up while processing information. This alarming statistic is equivalent to water usage roughly the same as a town of 30,000 to 50,000 people in the United States. These implications, given their significant influence on our resources and climate, cannot be ignored or brushed away. Along with this, videos generated by AI, which once looked bizarre, are now very close to realistic videos, and it is getting harder to differentiate between an AI-generated photo/video and a conventional one. This article has also delved into suggested regulatory codes in this area because there is a lack of a regulatory framework. It is important to note that AI has touched other spheres of life as it is being integrated into daily use items, from washing machines to as basic as toothbrushes. With the continuous increase in the number of users of these AI tools almost daily, it is pertinent to examine the impact it has on our ecosystem. Such technological systems are here to stay, and it is in our hands to use them mindfully so that the best possible outcome of them can be utilised.

II. POSITIVE IMPACTS OF AI

Artificial Intelligence is a brilliant technology in today's world, which enables us to generate ideas at our fingertips, and it is fascinatingly good at that. A wide array of tools is at our disposal, like Chat GPT, Gemini, Perplexity AI, and Microsoft Co-Pilot, which are some of the popular ones, but there are endless tools that are in the market currently, and they are only increasing by the day. The positives of AI are endless and can be seen in our day-to-day lives, considering how it is really helpful to students, teachers, engineers, doctors, scientists, mathematicians, and just about every major job profile. The use of Artificial Intelligence is now widespread. Its impacts on various sectors include:

2.1. Medicine and Healthcare

AI has helped in giving an initial diagnosis to people by examining their blood reports and symptoms. The latest model of ChatGPT even claims to detect cancer and other health risks early.[3] In a New York Times article, which was based on a

[2] Zoe Kleinman & Brian Wheeler, "*Concern UK's AI ambitions could lead to water shortages*", *BBC News*, Feb. 7 2025; *available at* <https://www.bbc.com/news/articles/ce85wx9jjndo> (last visited on October 21, 2025).

[3] The Times of India Tech desk, "ChatGPT-5 can now detect cancer and other major health conditions, claims OpenAI", *The Times of India,* published on August 9, 2025; *available at* https://timesofindia.indiatimes.com/technology/tech-news/chatgpt-5-can-now-detect-cancer-and-other-major-health-conditions-claims-openai/articleshow/123188307.cms (last visited October 21, 2025).

small study, it was also found that AI did better than doctors at detecting the illness, according to the case report and diagnostic case histories.[4] In a latest development, Google's CS2-Scale 27B foundation model has created a novel hypothesis for the detection of cancer cell behaviour by recognizing its patterns[5], which is a great step forward for using AI in medical sciences to help find cures for diseases.

AI can read multiple scans and reports at the same time, compared to a human doctor who can only tend to one patient at once. It can offer preliminary medical advice, helping people understand whether their symptoms are minor or require professional attention.

Since therapy is not accessible to everyone at all times, AI can step in to provide virtual assistance till the help can reach them. AI also holds immense potential in advancing neuroscience, which is one of the most complex domains in medical science. It has a capacity to store vast amounts of data and process multiple variables simultaneously, and also recognise new patterns which can help us analyse the neurological data at a scale and speed that is not possible for humans. Even an individual who has high intelligence or strong memory cannot match the computational ability of these systems, which will enable researchers to provide a better understanding of the human brain, identify novel patterns in neurological disorders, and accelerate the discovery of new treatments and potential cures for various diseases. Lastly, AI integrated into surgical machines for complex operations can help in increasing accuracy, mitigating operational risks, and reducing human errors.[6]

2.2. Engineering/ Mechanical Field

AI-based CAD (Computer Aided Design) systems have increased efficiency and optimised product designs. It can remember long and complex formulas, various combinations at the same time, which can significantly reduce human efforts in time-consuming calculations. AI can code faster with fewer errors and detect bugs more efficiently than humans. Mark Zuckerberg has even gone on to say that in

[4] Gina Kolata, "A.I. Chatbots Defeated Doctors at Diagnosing Illness," *The New York Times*, published on November 17, 2024; *available at* https://www.nytimes.com/2024/11/17/health/chatgpt-ai-doctors-diagnosis.html, (last visited on October 20, 2025).

[5] The Times of India Tech desk, "Milestone for AI in science: Google AI generates cancer hypothesis later validated by scientists, says Sundar Pichai", *The Times of India*, published on 16 Oct. 2025 *available at* <https://timesofindia.indiatimes.com/technology/tech-news/milestone-for-ai-in-science-google-ai-generates-cancer-hypothesis-later-validated-by-scientists-says-sundar-pichai/articleshow/124599530.cms#:~:text=Google's%20advanced%20AI%2C%20C2S%2DScale,new%20pathways%20for%20cancer%20therapy.> (last visited on October 22, 2025).

[6] Jack Ng Kok Wah, "The rise of robotics and AI-assisted surgery in modern healthcare," 19 *Journal of Robotic Surgery* 311 (2025).

18 months, coding will be done by AI, it will be better than the work of most engineers[7]. AI has transformed the whole coding sphere which is also predicted to replace humans in the near future[8] except for the few areas where it is still lacking and is projected to eventually cover the gaps, making coding completely automated. It may as well be a good sign, as anyone would be able to code within minutes by giving prompts to these coding software and design webpages and sites as per their convenience, without having to pay a professional coder a lump sum amount of money, and hence becoming more accessible to people. AI is capable of solving complex computational problems by going through large amounts of data and information from various sources faster than humans, although exceptions are still there, but ongoing developments indicate a positive trajectory towards achieving it. Most importantly, it can automate mundane tasks for us. AI's predictive maintenance in GE Aerospace, which is applied to monitor over 44,000 in-service engines in real time, sensor/flight data, along with Machine Learning models, forecasts failures and optimizes inspections.[9]

2.3. Agriculture

AI helps in analysing the soil, crop, and weather data and suggests the crop that would be optimal as per the projected conditions and predictive patterns. Research in the Journal of Agriculture and Food Research has talked about leveraging data from IoT sensors and GPS to tailor recommendations for irrigation, fertilization, and pest control, reducing waste and optimizing resource use. This makes agriculture more efficient, environmentally friendly, and cost-effective. Machine learning models analyse large datasets to predict crop yields, identify diseases early, and enable data-driven farm management. Robotics automates labour-intensive processes like sowing, harvesting, and weeding, alleviating labour shortages and increasing operational efficiency.[10] In India, platforms like 'Kisan e-Mitra' has an integrated AI-chatbot for farmers to answer queries about farming

[7] Nandini Yadav, "Mark Zuckerberg says in 18 months coding will be done by AI, it will be better than work of most engineers", *India Today*, April 30, 2025; *available at* <https://www.indiatoday.in/technology/news/story/mark-zuckerberg-says-in-18-months-coding-will-be-done-by-ai-it-will-be-better-than-work-of-most-engineers-2717414-2025-04-30> (last visited on October 19, 2025).

[8] The Times of India Tech desk, "Bill Gates says AI today can replace human work, the most complex coding tasks", *The Times of India,* August 3, 2025; *available at:* https://timesofindia.indiatimes.com/technology/artificial-intelligence/bill-gates-says-ai-today-can-replace-human-work-the-most-complex-coding-tasks-but-it-is-not-/articleshow/123068497.cms, (last visited on October 24, 2025).

[9] Prasoon Verma, "AI for Predictive Maintenance in Manufacturing", *INSIA Blog*, June 4, 2025; *available at:* https://www.insia.ai/blog-posts/ai-predictive-maintenance-manufacturing (last visited on October 20, 2025).

[10] Nazish Aijaz, He Lan, Tausif Raza, Muhammad Yaqub, Rashid Iqbal, Muhammad Salman Pathan, "Artificial Intelligence in Agriculture: Advancing Crop Productivity and Sustainability", Vol. 20, 101762 *Journal of Agriculture and Food Research*, ISSN 2666-1543 (2025).

or the latest schemes like PM Kisan Samman Nidhi and National Pest Surveillance System, which is an AI-based platform that uses advanced data analysis to detect pest infestations and use of drones for detecting early signs of crop failure, irrigation, water stress or effective distribution of resources in the field.[11]

2.4. Education

AI has transformed how humans learn and get information forever. It can analyse the speed of learning, problem-solving, and concept grasping of students and accordingly design a tailored lesson plan that matches everyone's needs and abilities within the stipulated time. It can be used for research, managing data, generating ideas, and handling administrative tasks efficiently. It can also generate flashcards, quizzes, provide analogies, tricks for learning, and make concise study notes in an easier language that can be more helpful to students. Online teaching and learning platforms are already using AI to enhance learning and answer queries. AI can be asked any question at any time of the day, and it will provide a dedicated answer as per the query asked, which makes the learning more accessible and inclusive for everyone, especially those who face barriers to traditional educational resources or support.

2.5. Business and marketing

It is transforming almost all areas of business and marketing. Online shopping platforms like Amazon, Netflix, and Prime have already integrated AI in their user interface (UI), which can be used to surf through products effectively on their websites. They are using customer analytics to give targeted recommendations to their users. Machine learning can predict future marketing movements through analysing data of past and present, and give an effective marketing strategy for these brands. An article in The Washington Post discusses how AI is rapidly transforming India's vast call centre and business process outsourcing (BPO) sector, introducing powerful automation and AI tools that are fundamentally altering how customer service is delivered. AI-powered chatbots, voice assistants, and real-time coaching systems are now handling a large share of routine customer support interactions, providing companies with significant cost reductions, faster response times, and improved customer satisfaction.[12]

---

[11] Sakshi Kuchroo, "AI is sowing the future: Indian farmers embracing smart tech, but this is just the beginning", *Financial Express*, May 29, 2025; *available at:* https://www.financialexpress.com/artificial-intelligence/ai-is-sowing-the-future-indian-farmers-embracing-smart-tech-but-this-is-just-the-beginning/3861349/ (last visited on October 24, 2025).

[12] Karishma Mehrotra, "AI is transforming Indian call centers. What does it mean for workers?", *The Washington Post*, June 21, 2025, *available at* <https://www.washingtonpost.com/world/2025/06/21/india-ai-bpo-call-centers/> (last visited on October 20, 2025).

2.6. Law

In the field of law, tools like Chat GPT and Perplexity are helping make legal research easier by finding relevant case laws and precedents faster than conventional methods. SCC online and Manupatra have also added features like AI generated summary in their platforms to accelerate legal research. There are also tools like draft bots that use AI and standardised formats to draft applications, contracts, and pleadings. Though it would not replace humans, as AI is bound to make mistakes, as there have been instances where AI has generated non-existent case laws. Although information confidentiality between lawyer and client would be violated if sensitive information of the case and clients were fed to AI. The Indian judiciary and law enforcement agencies are also increasingly adopting artificial intelligence (AI) and digital technologies to enhance efficiency, accessibility, and decision-making across the justice sector. AI technologies, including machine learning (ML), natural language processing (NLP), optical character recognition (OCR), and predictive analytics, are being leveraged to automate administrative tasks, streamline case management, and support crime prevention. The e-Courts Project Phase III, for instance, incorporates AI tools for smart scheduling, backlog reduction, and overall optimization of judicial processes, enabling faster and more effective case handling.[13] Along with this, the Supreme Court Portal Assistance in Court efficiency (SUPACE) is an AI-based tool that is still in the development stage, aiming to develop a module to understand the factual matrix of cases with an intelligent search of the precedents, apart from identifying the cases[14]

2.7. Governance

AI can be used to holistically and effectively govern a diverse set of populations, as evident through steps in that direction by governments around the world who are actively showing interest in integrating AI in our day-to-day governance. It can automate mundane and repetitive administrative tasks, which will improve the productivity of the overall structure of government. AI can help us formulate policies that are based on comprehensive data and a long-term understanding of the implications of these policies. It can also help in effective decision-making by the government and improve Information management.[15] Addressing grievances can be optimized through virtual chatbots and assistants. AI strengthens law

[13] Press Information Bureau Research Unit, "Digital Transformation of Justice: Integrating AI in India's Judiciary and Law Enforcement," (Ministry of Law and Justice, Government of India, February 25, 2025).
[14] Press Information Bureau, "Use of AI in Supreme Court Case Management", (Ministry of Law and Justice, Government of India, March 20, 2025).
[15] OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* (OECD Publishing, Paris, 2025).

enforcement by enabling predictive policing, real-time crime mapping, and facial recognition-based surveillance.[16]

2.8. Transportation and logistics

There has been a surge in self-driving vehicles from cars, trucks, planes, and just about any vehicle. It has also been integrated with AI technology, which monitors real-time surrounding areas for any objects or people, analyses the traffic conditions to choose the fastest route to reach the destination, makes decisions on how to drive the vehicle and follow the safe speed limit, and finally arrives at the destination safely and securely. Companies like Tesla, Waymo, and Cruise are heading this revolution in self-driving cars. Autonomous vehicles equipped with artificial intelligence can provide safe and reliable transportation for persons with disabilities, senior citizens, and individuals experiencing temporary impairments, whether due to cognitive challenges, mental health conditions, or intoxication. The global Automotive Artificial Intelligence (AI) Market size was valued at USD 4.29 billion in 2023, and is predicted to reach USD 25.78 billion by 2030, with a CAGR of 29.2% from 2024 to 2030.[17] AI can also ease traffic management by processing large amounts of data gathered through all these years of mapping technology and predict better routes, reduce congestion on roads, optimise vehicle performance, and help in suggesting better urban planning or solutions where there are constant traffic jams. It can also be very helpful in logistics, which is closely related to the transportation of goods and services, be it within the boundaries of a country or beyond them. AI can aid the supply chain management industry to a great extent by conducting high-volume data processing.

2.9. Media, Art, and Entertainment

There are countless tools at our disposal today, which enable us to create anything from videos, photos, text, music, and visuals with little to no production cost. This can be really helpful for artists who are just starting and may not have a big budget or support to fuel their ideas. In this new age of digitalisation and artificial intelligence, aspiring creators in this field can now use AI to execute their ideas with minimal production cost as compared to a big-budget movie. The use of AI in this sphere is evident from many commercials now being AI-generated, and there have been some recent movies that use AI along with CGI to execute their story lines. This has not only reduced the production cost but also made it more efficient. From choosing scripts that are more likely to generate revenue to editing

[16] Drishti IAS, "Harnessing AI for Governance", Feb. 11, 2025; *available at* https://www.drishtiias.com/daily-updates/daily-news-editorials/harnessing-ai-for-governance (last visited on October 24, 2025).

[17] Next Move Strategy Consulting, *Automotive Artificial Intelligence Market Report*, Report Code: AT357, Automotive & Transportation Industry Report, Sept. 25, 2025, *available at*: <https://www.nextmsc.com/report/automotive-artificial-intelligence-market> (last visited on October 20, 2025).

and making music for the movies[18], AI is doing it all. Major streaming platforms are leaning more towards the use of generative AI to reduce production costs and increase profits by using AI-generated characters rather than actual actors to play the part. It will immensely transform how the entertainment industry is viewed in the coming decade, as a rise in AI-generated content will be more prominent and undetectable, and it has already begun. This is the most controversial sphere where there hasn't been an open view on integrating AI, as there is a risk of deepfakes and spreading of misinformation, which puts us in an ethical dilemma about whether one must use AI in the field of entertainment or not.

2.10. Space exploration

Outer space is such a vast field where knowledge remains limited, and continued efforts are being made to discover the unknown and unexplored aspects of our universe. Space agencies around the world are using AI to explore space. AI not only helps in satellite imaging, which can detect asteroids, analyse planetary surfaces, predict events like meteor showers, navigate in space, but also can travel far to the ends of the galaxy for further space exploration, which is something that is constrained due to limited human capacities. However, AI can increase the efficiency of our resources and explore safely. NASA (National Aeronautics and Space Administration) is already using AI in various areas of its upcoming missions, from mission planning software like ASPEN mission planner, AWARE (Autonomous Waiting Room Evaluation), CLAP (Coverage Planning & Scheduling), to environmental monitoring and analysis. NASA also uses AI tools to organise data and automate tasks, and they aim to further integrate AI into more aspects of space exploration, from deep space missions to sustainable solutions for planetary exploration.[19]

III. NEGATIVE IMPACTS OF AI

The advantageous implications on the world are substantial, but the accompanying disadvantages warrant equal attention and cannot be ignored. The creators of OpenAI have started issuing statements regarding the need for regulations for AI to prevent it from destroying humans. Sam Altman himself calls for an international regulator to begin working on how to "inspect systems, require audits, test for compliance with safety standards, [and] place restrictions on degrees of deployment and levels of security" to reduce the "existential risk" such

[18] Siranush Andriasyan, "How Artificial Intelligence Is Used in the Film Industry", *Smart Click (2025)*; *available at* https://smartclick.ai/articles/how-artificial-intelligence-is-used-in-the-film-industry/#:~:text=Choosing%20the%20script%20that%20will,of%20resources%20in%20location%20scouting. (last visited on October 24, 2025).

[19] Kate Halloran, "NASA's AI Use Cases: Advancing Space Exploration with Responsibility", *NASA*, Jan. 07, 2025; *available at:* https://www.nasa.gov/organizations/ocio/dt/ai/2024-ai-use-cases/ (last visited on October 18, 2025).

systems could pose.[20] Godfather of AI, Geoffrey Hinton, has himself warned about the risks of rapid development and the large-scale unemployment that will be seen around the world due to AI usage.[21] Another pioneer in the field of AI who worked closely with Geoffrey Hinton in developing AI technology, Yoshua Bengio, has also warned about the risk of extinction by takeover of hyperintelligent machines that would sacrifice humans for their own survival.[22] Very recently, they have come together with other tech pioneers to urge for a ban on superintelligent AI.[23]

One must wonder why there would be such a need for demanding regulations when it is easing our lives? Accordingly, the negative impacts associated with the widespread use of AI must be examined to gain a greater insight into this issue.

There have been minimal to no transparency or safety measures undertaken while developing these AI tools and training them with data. Companies have been doing such training of AI models with data that is available online behind closed doors.

- Due to the data being available freely on public use platforms and search engines, it is inevitable that the biases that prevail in society would reflect in the responses of AI itself. There have been instances where AI has disproportionately profiled and categorised people on the basis of their race, gender, and other data available in its databases. These biases can be seen in hiring, lending of loans, and even law enforcement. The use of the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) tool, which employs an algorithm that analyzes various factors such as criminal history, social background, and personal characteristics to predict recidivism risk. In the case of State v. Loomis[24],

[20] Alex Hern, "OpenAI leaders call for regulation to prevent AI destroying humanity", *The Guardian*, May 24 2023; *available at* https://www.theguardian.com/technology/2023/may/24/openai-leaders-call-regulation-prevent-ai-destroying-humanity (last visited on October 20, 2025).

[21] Times of India Tech desk, "Godfather of AI Geoffrey Hinton warns: Real danger is not killer robots, but smooth-talking systems", *The Times of India*, Sept. 6, 2025, *available at* https://timesofindia.indiatimes.com/technology/tech-news/godfather-of-ai-geoffrey-hinton-warns-real-danger-is-not-killer-robots-but/articleshow/123679959.cms, (last visited on October 23, 2025).

[22] Marco Quiroz-Gutierrez, "AI Godfather warns humanity risks extinction by hyperintelligent machines with their own 'preservation goals' within 10 years", *Fortune,* published on 1 Oct. 2025; *available at* https://fortune.com/2025/10/01/ai-godfather-yoshua-bengio-ai-extinction-risks-openai-google-xai-anthropic/, (last visited on Oct. 23, 2025).

[23] US right-wing media figures, tech pioneers call for superintelligent AI ban, *The Economic Times,* Oct. 22, 2025; *available at* https://economictimes.indiatimes.com/tech/artificial-intelligence/us-right-wing-media-figures-tech-pioneers-call-for-superintelligent-ai-ban/articleshow/124733429.cms?from=mdr, (last visited on Oct. 23, 2025).

[24] *State v. Loomis*, 881 NW 2d 749 (Wis 2016).

it was found that the tool disproportionately labels Black defendants as high-risk. AI has also been found to be discriminatory towards women in its hiring practices; these tools systematically downgraded resumes submitted by female candidates.[25]

Now, one might argue that AI can just be trained not to have these biased approaches, but here comes the problem of the 'black box.'[26] which means that, as humans, only input can be provided by us to these systems and expect an outcome, but it is unclear how the AI system reached that conclusion, and there is no way to monitor or calculate what set of data was utilised for generating the result. This is because AI uses complex calculations using its database and algorithm, and when this data interacts with real-world inputs and situations, it is difficult to follow through as to how certain results were generated because there are intricate and complex calculations used by AI to deliver the results. It can be done for controlled and monitored searches on a very basic level, where the experts can track and calculate it to a certain extent, but it is not possible to do it for every single search, which is why AI scientists have been unsuccessful in eliminating such bias yet.

- Another very significant impact of misuse of AI would be on crimes and scams, the modern age has enabled hackers and scammers with tools through which they can be faceless while committing theft and when AI is put into the blend, it increases the danger ten folds, from use of deepfakes to clone faces and voices to developing malware and viruses with the help of AI itself that provides them with enhanced tracking techniques and automate multiple attacks at once with successfully evading our detection systems. It would be a nightmare for banking and financial institutions if such a theft were to occur. The number of cyber-attacks has already been on the rise in recent years. A cybercrime magazine reported that cyber-crimes are predicted to inflict damages totalling $9.5 trillion USD globally in 2024.[27]
- Another major impact is on our cognitive ability. Research was conducted by students of MIT, which used electroencephalography (EEG) to record the brain activity of groups to compare the neural activity of a group that used AI for an essay writing task and the other group, which did not use it. They assessed their cognitive engagement,

[25] Kadin Mesriani, "AI & HR: Algorithmic Discrimination in the Workplace", Cornell Journal of Law & Public Policy – *The Issue Spotter,* 21 Nov. 2024.
[26] Aleksandre Asatiani, Pekka Malo, Per Rådberg Nagbøl, et.al., "Challenges of Explaining the Behavior of Black-Box AI Systems", 19 *MIS Quarterly Executive* 259 (2020).
[27] Steve Morgan, "Top 10 Cybersecurity Predictions and Statistics for 2024", *Cybersecurity Ventures* Apr. 13, 2025; *available at* <https://cybersecurityventures.com/research/> (last visited on October 21, 2025).

cognitive load, and neural activations during the essay writing task. They also performed NLP analysis and interviewed each participant after each session. It was found that participants who used a large language model (LLM)/AI for these essay writing tasks showed less neural activity as compared to those who did not take help from these tools.[28] This study clearly shows how these AI tools on the surface reduce our workload but are making us dependent in the long term because then people would not use their own cognitive ability or trust their memories and experience and believe everything that these AI tools want them to believe, which will eventually reduce our critical thinking abilities and hamper our cognitive development.

- The jobs market is already been significantly impacted since the introduction of AI. It has automated a lot of mundane tasks and increased efficiency in offices, but has also led to people being laid off because their role is now being served by AI agents or tools. From big tech companies like Google, Microsoft, Meta, Amazon to Tata Consultancy Services (TCS), Accenture, and Tech Mahindra have laid off thousands of employees in order to cut the costs in salaries and invested more in AI platforms that reduce human errors and are also efficient.[29] An article by Goldman Sachs talked about how AI could increase unemployment in two ways: one being replacing human labour entirely, where they are no longer needed for those tasks, or by causing short-term job displacement till the time new jobs are created. Although they predict that employment growth will stem from technology-driven roles in the future, and they base their argument on how historically innovations also feared a permanent reduction in human labour, but that was proven unfounded with time.[30] Despite this outlook, even the temporary loss of jobs may push families and individuals into a downward spiral if they do not have resources to upskill themselves after already investing in their education. This loss of jobs is not limited to white-collar jobs but also creative jobs due to the use of generative AI.

[28] Nataliya Kosmyna, Eugene Hauptmann, Ye Tong Yuan, Jessica Situ, Xian-Hao Liao, Ashly Vivian Beresnitzky, Iris Braunstein & Pattie Maes, "Your Brain on ChatGPT: Accumulation of Cognitive Debt When Using an AI Assistant for Essay Writing Task" *MIT Media Lab* / arXiv, published on 10 June 2025; DOI:10.48550/arXiv.2506.08872.

[29] Mohit Pandey, "Biggest AI layoffs of 2025", *Analytics India Magazine*, Aug. 8 2025; *available at:* https://analyticsindiamag.com/ai-trends/biggest-ai-layoffs-of-2025,(last visited on October 20, 2025).

[30] The Goldman Sachs Group, "How Will AI Affect the Global Workforce?", *Goldman Sachs Insights,* Aug. 13, 2025, *available at:* https://www.goldmansachs.com/insights/articles/how-will-ai-affect-the-global-workforce, (last visited on October 20, 2025).

- India is a big market for these corporations; this huge population is willingly giving these companies data to train their models. India is often used as the target audience to gather data and train their new models. There are no strict privacy laws and Intellectual property rights laws regarding the usage of data by AI of users that supervise and hold these corporations accountable for not maintaining transparency as to how and where this collected data is being used. AI may not use the data verbatim but instead paraphrases it, which creates a potential loophole in copyright protection laws. These companies can easily evade liability through paraphrasing, asserting the absence of direct infringement.

- AI may also prove to be a dangerous tool in the hands of authoritarian governments, who may alter databases and manipulate elections, and increase polarisation. They may use such tools to develop autonomous weapons that can attack and target their enemies with precision. This can prove to be disastrous in the wrong hands.

- There is also unhealthy competition between companies like Open AI v. Deepseek and countries, mainly China and the USA, to develop the best model of AI before the other. These companies have invested billions of dollars in research and development of the most advanced system of AI. The race for leadership in AI is aggravating geopolitical tensions, restructuring alliances, and setting new benchmarks for technological superiority. As innovation in this sphere becomes closely tied to national security and economic policy, its impact and influence reach far beyond these two superpowers, compelling countries around the world to step in and adjust to this quickly evolving yet uncertain international landscape.[31] If China were to ultimately 'win' this AI race, the values that the RTAI (Real-Time Application Interface) system reflects are very much Chinese, whereas if the U.S 'wins' the values inculcated would very much be Western in nature. Because of this, the attempt to bring about safe and strong AI safety measures often breaks down at some stage as countries that are falling behind may, to impose their dominance, choose conflict to deter their rivals.[32] It can be observed that it is a race at this point as who will be pioneering AI by the end of this decade and even if the risks of unregulated development are right in front of us, they are not being acted upon actively because if one of these countries or companies stop or slow down the speed of innovation, the other will take over and threaten to dominate the geo-political sphere because technology is the new age weapon. This has led to a cut-throat

[31] Qutbah S. A., "AI Rivalries: Redefining Global Power Dynamics", *TRENDS Research & Advisory*, Feb. 16 2025

[32] Ross Gruetzemacher, Shahar Avin, James Fox, and Alexander K. Saeri, "Strategic Insights from Simulation Gaming of AI Race Dynamics", *Futures*, Vol. 167, 2025, 103563.

competition in which engineers and intelligent minds of our generation in the tech field are utilizing and focusing on this sphere of technology solely.

IV. IMPACT ON CLIMATE CHANGE

The most significant impact can be seen on the climate, and it is the least discussed. From semiconductor mining, which powers the AI chips, to large data centres that consume huge amounts of water, the impact of AI on the ecology is undeniable, yet the most sidelined.

- According to a report, the supply of copper in large quantities requires a robust supply of water. Around 1,600 litres of water are required to obtain the amount of copper found in a single medium-sized family car (19 kilograms).[33] Processing copper ore from a single mine can consume enough water every seven weeks to fill an 80,000-seat stadium.[34] Semiconductors are the hidden lifeblood of modern technology, embedded in everything from computers and phones to cars and washing machines. That means disruption to the semiconductor supply can have severe economic consequences.[35] PwC research projects the semiconductor industry will reach a value of $1 trillion just five years from now (in 2030), fueled by the growth of AI and the Internet of Things. Businesses cannot rely on future emissions reductions to protect them from climate risks and should prepare now to operate in a world in which critical commodities will be increasingly threatened.[36]

It is clear from such studies and reports that the production of semi-conductor that essentially provide the fuel to chips on which AI runs its functions, is costing the environment on a large scale, and instead of focusing on how to mitigate such risks, companies are more concerned with finding solutions as to how they can maintain a consistent supply of these chips without it getting affected by climate change. The following paragraph reflects the same: "Climate change could disrupt semiconductor production in many ways. For example, extreme weather can damage infrastructure, shut down plants, and play havoc with transportation and communication systems. Such harms could heighten geopolitical tensions, lift prices or constrict supplies of necessities from energy to insurance, and raise the cost of capital for businesses that are unprepared to adapt to a hotter world."[37] The

[33] Commonwealth Scientific and Industrial Research Organisation (CSIRO), cited in '*Water considerations for copper mining in the Americas*.'
[34] 'How can copper mines use less water,' Worley Engineering, 2023.
[35] Glenn Burm PwC Global Semiconductor Leader, Partner, PwC Korea
[36] Climate change threatens the world's most critical technology; PwC. (2025, July 8).
[37] Ibid.

mindset of these big companies and corporations is only to maximise profit even if it comes at the cost of the environment.

The electronics these data centers house rely on a staggering amount of grist: making a 2 kg computer requires 800 kg of raw materials. As well, the microchips that power AI need rare earth elements, which are often mined in environmentally destructive ways.[38] The second problem is that data centres produce electronic waste, which often contains hazardous substances, like mercury and lead.[39]

- The use of water-intensive cooling systems to prevent the systems from overheating in data centers is widely used to maintain the systems working day and night. The statistics as to the actual amount of water consumption in these data centers vary, but the latest approximate figure available is that large data centers collectively are consuming up to 5 million gallons per day, which is equivalent to the water use of a town populated by 10,000 to 50,000 people[40].

Together, the 5,426 data centers consume billions of gallons of water annually. One report estimated that U.S. data centers consume 449 million gallons of water per day and 163.7 billion gallons annually (as of 2021).[41] In the United States, about 2,600 data centers are clustered around Arizona, Dallas, the San Francisco Bay area, and Los Angeles, according to a 2021 report by the U.S. International Trade Commission[42]. All told, a mid-sized data center consumes around 300,000 gallons of water a day, or about as much as 1,000 U.S. households, says Shehabi of Lawrence Berkeley National Laboratory. Their direct, on-site consumption ranks data centres among the top 10 water users in America's industrial and commercial sectors.[43] All this startling evidence is still not enough as data centers are only projected to grow in terms of number and size, which will eventually lead to larger consumption of water for cooling down and use more energy. These water extractions cause strain on the local water sources, and in areas such as the western United States, home to data centers operated by large tech companies,

[38] United Nations Environment Programme, "Navigating New Horizons – A Global Foresight Report on Planetary Health and Human Wellbeing", produced by UNEP in collaboration with the International Science Council.
[39] United Nations Environment Programme, "AI has an environmental problem. Here's what the world can do about that", United Nations Environment Programme (UNEP), 21 Sept. 2024.
[40] Miguel Yañez-Barnuevo, "Data Centers and water consumption", Environmental and Energy Study Institute (EESI), 25 July 2025
[41] Ibid.
[42] Brian Daigle, "Data Centers Around the World: A Quick Look", United States International Trade Commission Executive Briefings on Trade, Office of Industries, May 2021.
[43] Michael Copley, "Data centers: Backbone of the digital economy face water scarcity and climate risks", NPR report, Aug. 30, 2022.

this poses a threat to an already drought-stricken region. The cost of installing and running these large air conditioning and air movement systems presents even more downsides for doing data center cooling the traditional way.[44] GPT-3, an AI model, is estimated to consume 500 ml of water per 10-50 responses. When multiplied by the billions of its users, the total water footprint of AI becomes enormous. By 2027, global AI demand is expected to account for 1.1 to 1.7 trillion gallons of water withdrawal, more than 4-6 times the total annual water withdrawal of Denmark.[45]

Microsoft's global water use soared by 34% while it was developing its initial AI tools, and a data centre cluster in Iowa used 6% of the district's water supply in one month during the training of OpenAI's GPT-4.[46]

An important pointer about this water consumption is its reliance on municipal water supplies. When large amounts of municipal water is diverted to data centers within a city's water district, the overall demand increases and as a result, the residents would have to pay more for their basic need of water even if their usage has not increased. The rise in cost brings little to no improvement in their quality of life because the benefits generated by these data centers are economic in nature, which has little correlation to their life.

The energy consumption of these AI systems is also huge. To keep these models available and operational at all times, big amounts of energy is required. It is estimated that data centres accounted for around 1% or 2% of global electricity demand in 2020. All that processing power generates lots of heat, so data centres must keep cool to prevent damage.[47] A request made through ChatGPT, an AI-based virtual assistant, consumes 10 times the electricity of a Google Search, reported the International Energy Agency. While global data is sparse, the agency estimates that in the tech hub of Ireland, the rise of AI could see data centres account for nearly 35 per cent of the country's energy use by 2026.[48] It is also projected that by 2050, the total amount of e-waste generated will have surpassed 120 million metric tonnes.[49]

---

[44] Matthew T. Ziegler,"The World's AI Generators: Rethinking Water Usage in Data Centers to Build a More Sustainable Future", *Lenovo Story Hub*, Mar. 22, 2024.
[45] Wesley Spindler, Luna Atamian Hahn-Petersen, and Sadaf Hosseini, "Why Circular Water Solutions Are Key to Sustainable Data Centres", World Economic Forum, Nov. 7, 2024.
[46] Zoe Kleinman & Brian Wheeler, "Concern UK's AI ambitions could lead to water shortages", *BBC News*, Feb. 7 2025; (last visited on October 21, 2025).
[47] Masaō Ashtine and David Mytton, "The True Cost of Water-Guzzling Data Centres", University of Oxford.
[48] Supra at 40.
[49] "A New Circular Vision for Electronics Time for a Global Reboot" by World Economic forum and the World Business Council for Sustainable Development, published in January 2019.

By looking at all this data and research, it is fairly evident that the use of AI is contributing significantly to the environmental problems, and it is not sustainable for the environment. From large energy and water consumption to mining of rare minerals to producing components for chips that run AI, it all leads to adverse effects on our environment. The carbon footprint of AI is only increasing by the day as more and more users are joining in, to the point that these systems are lagging and taking longer than usual to respond due to heavy requests on their servers. This shows that not only is AI becoming a regular search engine alternative, but also the catastrophic effects due to its usage over time, which will lead to devastating effects on our ecological systems. The world was already battling climate change before the advent of AI, but now, after looking at all the data and analysing the statistics, the process appears to have sped up, contributing to the continuous rise in global temperatures and extreme weather events. The usage of AI has put heavy strains on water resources, especially in the regions where these large data centre facilities are located. The area surrounding these complexes has complained of disruption in the supply of water. Along with this, the mining of rare earth minerals in an unsustainable manner will deplete these natural resources and lead to more environmental degradation. All this will also inevitably result in the generation of huge amounts of e-waste, which may contain hazardous materials like lead and mercury, and can further contaminate soil and water if not disposed of properly. Serious and effective measures are required on our part to curb these impacts and mitigate the effects of this on our climate.

V. Positive Impacts of AI Suggested Regulation Measures

The development in this field is going at an exponential speed and there are no regulations or framework in place to control its usage and development. One of the pioneers of AI, Yoshua Bengio said that 'A sandwich has more regulations than AI' (currently).

One of the difficulties in framing regulations for AI is that all the potential risks of AI are not fully understood. A better clarity is needed on the kind of risks that are expected to arise for developing a framework for regulating the same. It is also one of the fields that is growing at an unprecedented pace; it is a challenge to keep up with evolving changes, which can be seen almost every day. The framework has to be dynamic enough to integrate successive changes and advancements in this rapidly accelerating technology. Some of the suggested regulations and proposed solutions for the same would include:

- AI can be used to control AI, similar to how peer-to-peer checks work in a classroom setting. An AI can be developed to maintain the checks and balances that ensure transparency of the AI systems because it is too complex for humans to know and monitor exactly how it is using algorithms and databases to generate certain results. Such delegated duty on AI itself, which would be of the kind that would be put in place to

exclusively supervise and, in a way, decentralise regulation in technology. These systems will be designed to monitor and correct through internal checks and follow regulations. This solution was inspired by one of the pioneers of AI, Yoshua Bengio, who talked about a supervisory AI model because humans have limited capability in tracking the rapid and numerous calculations that AI systems make, but another AI could keep supervision that will be embedded with stricter morals.

- Stricter enforcement of compliance with the rules and regulations that will be developed through the framework. This framework has to be ideally globally applicable because AI does not have boundaries, it is borderless and accessible to everyone who has the internet.
- A risk management process can be developed that can detect threats like cybersecurity breaches, financial threats beforehand, and warn us to be prepared with precautions. It can also be used in a way to have an impact assessment of a new LLM model that may have been newly launched in the market and a prior vetting of this model/tool can be done so as to reduce any future misuse and danger.
- An international level cooperation would be required to frame these regulations and to keep the systems accountable and transparent
- An emerging field of AI ethics can be popularised to include more intelligent people who will represent their respective countries and brainstorm ideas along with providing valuable insights for regulating measures.
- A limit on usage of AI can be set, which may be a monthly or weekly limit that deters excessive use of AI and energy consumption. Although this is not possible currently because of the current revenue models, it can be a consideration for the future.
- The European Union (EU) AI regulation framework can be used as a basis for forming these regulations. It has a tiered system that categorises risks associated with AI into categories like unacceptable risk, high risk, minimal risk and low risk. The EU has categorised these as unacceptable risks and banned AI applications which include:

1. Cognitive behavioural manipulation of people or specific vulnerable groups
2. Social scoring AI which classifies people based on behaviour
3. Socio-economic status or personal characteristics
4. Biometric identification and categorisation of people

5. Real-time and remote biometric identification systems, such as facial recognition in public spaces[50]

- An aim to slow down innovations in AI would also be helpful because such progress is being made at a remarkable speed and yet caution should be maintained with regards to this fairly novel technology.
- AI should be majorly implemented and must be used for the benefit of society in the fields of medicine, space, technology, complex mathematical calculations, science, areas that actually require its computational abilities.
- China's trail of setting up data centres underwater[51] can also provide a good solution for water usage which can significantly bring down the usage of water for cooling down systems as the surrounding seawater naturally facilitates temperature regulation, eliminating the need to transport water from external sources.
- Other solutions for reducing water consumption in data centers include the use of:

1. **Direct water-cooling system**-uses loops of warm water to cool data centre systems in a circulatory manner, making the process more efficient. Compared to traditional air cooling, this method can be seen to have a 40% reduction in power consumption and improves heat management mechanism up to three and a half times.[52]
2. **Closed-loop cooling systems** use techniques such as wastewater recycling and rainwater harvesting which are already efficient ways to save water and hence, they tend to reduce the use of freshwater for cooling purposes. With a potential to save up to 50-70% of fresh water where these systems are implemented.[53]
3. **Free cooling system** takes advantage of naturally cold outdoor air. Instead of using air conditioners that heavily use power and also emit greenhouse gasses, data centres can pull the cold air from outside and use it to then cool the heat generated from the equipment's. Data centers

[50] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). July 12, 2024.
[51] You Xiaoying, *China Powers AI Boom with Undersea Data Centers*, *Scientific American*, July 16, 2025, available at: <https://www.scientificamerican.com/article/china-powers-ai-boom-with-undersea-data-centers/> (last visited on October 24, 2025).
[52] *Supra* at 45.
[53] *Supra* at 46.

must be located in cooler climate regions for this method to be effective.[54]

4. **Air cooling systems** involves air conditioning, vents and tubes that remove heat when produced by computer chips as they process data and AI requests. This method is suitable for areas where electricity is relatively cheaper and water supply is limited.[55]

VI. CONCLUSION

In conclusion, AI is a growing field of technology that holds our future in its hands. It seems like the world is prioritising quickness over quality and speed over experience in today's world. A prudential course must be maintained to ensure steering on a safe pathway and use AI for public good and welfare. As the duration of completing tasks by AI is getting faster every day, in formulations of such regulatory frameworks for this technology, caution must be exercised to not over regulate and stifle technological development and water down the entrepreneurial environment for innovation. Proportionate and necessary regulations must be put in place to address the growing concerns of climate change and potential misuse of this technology, which is freely at everyone's disposal. Every technology has its advantages and disadvantages, but it is our responsibility to maximise advantages and encourage positive uses of AI. It is a remarkable technology with a potential to be a boon for humanity, and it is our stewardship that decides its fate which is inseparable and linked with ours too.

[54] *Supra* at 41.
[55] *Ibid.*

DIGITAL EMPOWERMENT AND WOMEN'S ENTREPRENEURSHIP IN RURAL HARYANA

Dr. Saumya Sharma [*] ***& Ms. Shikha Yadav*** [**]

ABSTRACT

The paper will discuss how women-led startups emerge in rural Haryana and how law, technology, and social norms are interconnected. Based on qualitative interviews (n = 32) in six districts, the research evaluates driving forces, impediments, and regulatory experience of digital entrepreneurship. Technology is seen as a route to markets and a landscape of danger. Its gains have been determined by access to digital technologies, institutional endorsement, and social acceptance. Five dimensions of interaction with each other are identified as Digital Access, Institutional Support, Regulation, Social Legitimacy, and Resilience using reflexive thematic analysis, and bring together to create the result of empowerment. The article contributes to the discussion of the law of technology, gendered entrepreneurship, and sustainable development by proposing a gender-sensitive regulatory approach that emphasizes assisted compliance, privacy protection, and district-level Incubation. Results support the idea that women's digital entrepreneurship will succeed when technology and regulation develop together to enable inclusive participation.

I. INTRODUCTION

The startup ecosystem in India is growing and becoming more sophisticated[1], with more women founders entering the value chain. However, this visibility[2] is not even inherently so[3], especially in rural locations where infrastructure, financial, and network access are limited[4], and norms on mobility and legitimacy remain important to entrepreneurial decisions. The rural Haryana serves as a prism through which the effects of digital technologies and regulatory frameworks can be analysed and the barriers reduced or reproduced. The focus of this inquiry lies in a broader conversation about law and technology, where law is not just a frame but an enabler of access, trust, and participation. The connection between legality and digitalisation is even stronger in rural environment, where first- generation

[*] The author is an Associate Professor at the Department of Management and Commerce at The NorthCap University and can be reached at saumyasharma@ncindia.edu

[**] The author is an Assistant Professor at the Department of Management and Commerce at The NorthCap University and can be reached at shikhayav@ncuindia.edu

[1] Global Entrepreneurship Monitor, *Women Entrepreneurship Report 2023–24* (2024).

[2] Cherie Blair Foundation for Women and Reuters, *How Technology and Trust Are Failing Women Entrepreneurs* (2025).

[3] World Bank, *Women, Business and the Law 2024* (2024).

[4] OECD, *The Missing Entrepreneurs 2023: Policies for Inclusive Entrepreneurship* (OECD Publishing 2023).

entrepreneurs need to deal with new technologies like the internet and Aadhaar while also having to face the rigors of the regulatory landscape.

II. Literature Review

2.1. Global Momentum and Lopsided Indian Participation

Entrepreneurship by women is a phenomenon experienced across the globe, and women are becoming business starters and entrepreneurs. The Global Entrepreneurship Monitor (GEM)[5] Reports of 2024 explain that despite the increase in the total number of female entrepreneurs, the situation differs according to the region and the industry. The activity of female entrepreneurship is often concentrated in micro and informal sectors in India, where there is a significant percentage of female entrepreneurship activity with little access to finance, assets, and networks[6]. These restrictions are likely to freeze the growth processes and make them less scalable. In addition, their culture and social norms may ostracize women, and this remains a self-perpetuating cycle of exclusion. To build inclusive entrepreneurship policies, the necessary steps that need to be undertaken include ensuring that underrepresented founders, in particular women, youth, rural founders, and locked-out-of-mainstream-markets founders, receive the means to apply their entrepreneurial ideas to practice. It emphasizes the significance of certain support mechanisms that might be offered to women to help them penetrate the entrepreneurial landscape.

2.2 Digital transformation: Enabler and Divider

The new digital technologies have a two-fold impact on the entrepreneurial landscape. Digital platforms are also very important in lowering transaction costs[7] and geographical barriers, which, in turn, allow micro-entrepreneurs to reach larger markets, but they also exacerbate existing disparities. There is a long-standing mobile internet gender gap in South Asia[8], and many factors contribute to this situation, with affordability, safety reasons, and different degrees of digital literacy being the primary ones. It is based on these differences that specific interventions demonstrate that assisted onboarding, vernacular-language interface, and peer-mentoring programs can be adopted[9] to effectively increase the adoption of digital tools among women. In addition, the intersection of technology and gender has been identified to portray that women are more likely to encounter further challenges over the internet, such as harassment and online

[5] Global Entrepreneurship Monitor, *Women Entrepreneurship Report 2023–24* (2024).
[6] OECD, *The Missing Entrepreneurs 2023: Policies for Inclusive Entrepreneurship* (OECD Publishing 2023).
[7] UNCTAD, *Digital Economy Report 2025* (United Nations 2025).
[8] GSMA, *The Mobile Gender Gap Report 2023* (2023).
[9] LEAD at Krea University, *Reducing Rural Women Entrepreneurs to Digital: The Experience of NRLM Pilots* (2023).

violence, and so this may discourage them from using any form of digital platform.

2.3. Legal Regulations of the Digital Space

Digital commerce is based on trust. In this context, legal literacy becomes a critical yet often overlooked factor. For many rural women entrepreneurs, compliance is mediated through intermediaries such as agents or family members, which creates dependency and reduces autonomy. This raises concerns about whether formal legal frameworks, though neutral in design, may produce unequal outcomes in practice. Therefore, the effectiveness of digital regulation must be assessed not only in terms of statutory design but also in terms of accessibility and usability. The Digital Personal Data Protection Act, 2023 (DPDP)[10] of India specifies the standards for consent and data processing (MeitY, 2023), which will impact small businesses that handle personal data. Cyber safety and redress are important issues, as women entrepreneurs are particularly vulnerable to online harassment, fraud, and impersonation[11], which may discourage visibility. In the meantime, compliance regimes[12] (GST registration/returns, MSME Udyam) can impose an unfair burden on micro founders who lack assisted e-governance.

2.4. Policy Ecosystem and State Capacity

A set of mechanisms has enabled entrepreneurship, but the Startup India Action Plan (2016) has paved the way. Both of them are assisted at state levels by means of procurement preferences, incubator connection, or seed grants[13]. However, when the global benchmarking studies and the Sustainable Development Goals (SDG) Index in India [14] are compared, it becomes possible to state that the outcomes of both the actual performance and the set statutory regulations vary considerably. As an illustration, the implementation of digital payment solutions (UPI)[15] and smartphones is associated with an increase in the performance of MSMEs located in metro areas, which implies that the use of technology can bring substantial returns to a local economy.

2.5. Rural Haryana: Evidence-based on Barriers and Enablers

Rural Haryana is the best place to study the barriers to female entrepreneurship. Research also reveals that barriers that complicate the life of aspiring women

[10] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023* (Act 22 of 2023).
[11] T Kapoor, 'Feminine Cybercrime in India: What and How to Do About It' (2023) 5(2) *International Journal of Indian Legal Research* 45.
[12] World Bank, *Digital Compliance and Small Businesses* (2024).
[13] Government of India, *Startup India Action Plan* (2016).
[14] NITI Aayog, *India Index and Dashboard of SDG 2024–25* (2024).
[15] '73% of MSMEs Report Seeing Business Growth Through Digital Adoption' *Economic Times* (15 March 2025).

entrepreneurs are literacy barriers, restrictions in movement, and unawareness in the regulations[16]. Peer networks and Self-Help Groups (SHGs) now play a significant role as scaffolds to aid in learning, sharing risks, and the emergence of a sense of group empowerment. A recent study also discovered that the primary predictors of the sustained adoption of digital payment systems among women micro-entrepreneurs in the region are perceived usefulness, trust in digital platforms, and enabling conditions[17]. The theme of this literature is that proportional regulation/safety-by-design thinking and district-level incubation programs are the main point that connectivity will turn into real empowerment of women in the digital entrepreneurship sector.

2.6. Intersectionality and Women-Led Startups

Moreover, the intersectional lens offers valuable understanding into how multi-layered identities, including caste, class, and place can influence women's entrepreneurial lives. Studies show that the opportunities and achievements for women entrepreneurs from marginalised background groups might be restricted due to layered challenges .Matching interventions and enabling inclusive contexts that provide support and encouragement for all women entrepreneurs, especially in rural settings, is vital to consider this multidimensionality.

2.7. Role of Education and Skill Development

Education plays a crucial role in helping women successfully navigate the entrepreneurship landscape. Research suggests that better access to education and skills-based training focused on entrepreneurial needs could boost female participation and success in rural areas. Programs that provide digital literacy, financial management, and marketing education are very effective for enabling women to utilize technology effectively and grow their business. This literature review offers a comprehensive view of the various dimensions of challenges and opportunities faced by women entrepreneurs in rural Haryana; highlighting the need to take a holistic approach that combines technology, legal provisions, and social empowerment programs.

2.8. Theoretical Framework

The analysis integrates the feminist institutionalism with Sen's Capability Approach (including freedom, functioning, and conversion factors). This lens understands how formal rules such as data protection, cyber safety and MSME formalization are shaped by the other more informal norms, including gendered

[16] World Bank, *Women's Empowerment in South Asia* (2023).
[17] Women Entrepreneurship Development in India: Challenges and Suggestions (IJRASET, 2025).

legitimacy, family approval, and mobility. Value of technology can be thus moderated by regulatory clarity, assisted compliance and social acceptance.

2.9. Research

in the community. The final result is manifested in psychological, social, and financial independence.

Importantly, empowerment is not a static end-state but a self-reinforcing process. As women gain confidence and experience, they are more likely to engage in peer learning by mentoring new entrants and sharing knowledge within their communities. This growing confidence also strengthens their ability to negotiate, make independent decisions, and expand their business activities. Visible success further contributes to family acceptance, which in turn reduces resistance and encourages sustained participation. Empowerment, therefore, operates as part of a cyclical feedback loop, where individual gains reinforce broader social legitimacy and resilience, ultimately sustaining and expanding the entrepreneurial ecosystem. Here, empowerment does not happen in a vacuum; it is a cyclical process that fosters social legitimacy and resilience by establishing a self-reinforcing feedback loop within the ecosystem.

2.10. Cross-Cutting Engine: Resilience and Adaptation

The central player in the framework is found to be linked horizontally with nearly all nodes. It is a reflection of women's strategic coping, learning from the hard times and adaptation by peers.

Resilience and adaptation act as a cross-cutting mechanism between all the elements of the framework. Rather than a fixed set of characteristics, resilience is a process in which women learn to cope with constraints, adapt to negative experiences, and evolve their coping strategies as they go. This involves learning from one another through SHG networks, coping with online fraud and/or harassment, and changing the business practices – change to a safer platform or payment system. These processes can lead to challenges being recontextualized into learning opportunities and to the sharing of learning opportunities within peer networks.

Themes are not presented in a linear order in the relationships shown in Figure 1 but they are dynamically connected. Access to the digital, institutional support, regulatory frameworks and social legitimacy all help to empower, but linkages between them vary by context. Resilience is spread out across these domains and is able to maintain entrepreneurial activity despite the strength of any one domain. Empowerment in turn reinforces access, the support network, and social acceptance for other people, as successful entrepreneurs can become local mentors or role models. The framework is therefore more of a process, and one that is iterative and interdependent, in which the trajectory of progress is a result

of ongoing interaction between individual agency and structural conditions. Female champions could be female trainers and SHG leaders, which could lead to greater access and support. Weakness in one area of the empowerment chain can disrupt the overall chain of empowerment (Cyclical Dependency). This systemic picture highlights that the digital empowerment process is an ecosystem, and that the infrastructure, institutional design, simplified policies and cultural change should interplay.

III. Observations

Three cross-cutting insights were highlighted. To begin with, technology as ambivalent infrastructure: platforms such as WhatsApp Business and Instagram were more accessible, but connectivity issues and fraud concerns limited their use. Women recorded learning curves in image quality, catalog maintenance, and customer feedback after they finished household chores, usually at very late times, since there was not enough bandwidth to support such activities.

Second, control as a guarantee and fear: MSME/GST formalization was a guarantee of legitimacy and access to procurements; however, unfamiliar portals, lengthy English-language forms, and the need to use intermediaries added extra costs and led to less confidence.

Third, social legitimacy as a conversion factor: when family and peer acceptance were high, women tried out more digital tools; when standards were strict, movement and presence were constrained, and it did not matter whether one had an internet connection.

There was theme interplay: a participant with modest digital skills and strong support from SHG managed to navigate e-commerce after a district-level workshop on the topic, while another with good connectivity did not want to buy online because of harassment incidents. Assisted e-governance camps and handholding by incubators or NGOs in several districts helped with first-time registrations and UPI adoption.

3.1. Implications of Policy and Law

To be gender responsive a regulatory agenda ought to:

(a) make safety by design (privacy defaults, easy reporting, fast redress) in platforms that are commonly frequented by women micro entrepreneurs;

(b) implement aiding compliance with the mobile one-stop camp in vernacular interfaces of Udyam/GST;

(c) expand proportional compliance to minuscule businesses; and

(d) institutionalise district Women Tech Hubs connecting SHGs to legal, fintech, logistics, and market support. Compliance with DPDP regulations and state startup policies may enhance trust and adoption.

IV. Conclusion

Female entrepreneurs in the rural Haryana are resourceful. Digital access allows regulation, institutional handholding and social legitimacy to cooperate, thereby achieving empowerment. The evidence shows that a more systemic approach is needed rather than technology: a safe and private Internet, streamlined and supported formalization processes, and community support and mentoring to build sustainable opportunities from Internet connectivity.

Mixed methods design of future research can help quantify the effect of assisted compliance on formalization and revenue outcomes in a meaningful way. It can also benefit from longitudinal cohort studies that follow indicators of resilience over time (e.g., fluctuations in earnings), as well as digital confidence. Furthermore, the study of privacy defaults and seller verification procedures at the platform level would yield insights on their impact on women's perceived safety in digital platforms. Last but not the least comparative analysis of Haryana with other states can help identify features of policy that might be best suited to predicting and encouraging inclusive entrepreneurial development.

E-GOVERNANCE POLICIES: A CASE STUDY OF RAJASTHAN IN THE POST-COVID PERIOD

Somya Tewari [*] ***& Swetanka*** [**]

ABSTRACT

The world has seen a 360-degree change today in the way it used to run in the pre-COVID era. The implementation of government schemes through E-services is one of the many changes that the COVID-19 pandemic has brought about in various industries. Like many other Indian states, Rajasthan has embraced this digital revolution to provide effective and easily accessible governance both during and after the outbreak. This critical analysis assesses the efficacy of Rajasthan's post-COVID-19 e-governance model. The objective of this research is to gather information from the residents of Rajasthan regarding the effectiveness of the e-governance services. The availability and willingness of the people to use the new system is paramount to the success of the government's e-governance model. It has to be analyzed whether the potent Information and Communication Technology (ICT) mechanism can effectively encourage residents to actively participate in accessing government services. Analyzing data such as user counts, services provided, and citizen satisfaction levels may provide insight into the effectiveness and impact of the modifications implemented.

I. INTRODUCTION

The government of Rajasthan has designated IT and ITeS as a key focus area for the expansion and advancement of e-governance. The State Government is making every effort to implement Government schemes through E-services across the entire state, encompassing all sectors, to offer the general public (both in urban and rural areas) hassle-free, transparent, and efficient services. The government of Rajasthan established the "Computer Directorate" in 1987 to facilitate information technology initiatives and to make it organized, structured, and equitable. This was renamed in 1997 as the Information Technology Department. Further, the government of Rajasthan renamed the department as the Department of Information Technology & Communication, or the "DoIT&C," which is working to put technology to its highest and best use throughout the state of Rajasthan, Government Departments/Autonomous Bodies to improve the administration of State programs and services. They provide and facilitate guidance on technical matters to Departments, vetting of various IT projects, and to further the objective of taking the Department to achieve the IT Road

[*] The author is an LL.M. student at the Faculty of Law, Banasthali Vidyapeeth, and can be reached at tewarisomyatewari@gmail.com.

[**] The Co-author is an Assistant Professor at the Faculty of Law, Banasthali Vidyapeeth, and can be reached at swetanka@banasthali.in.

Map."[1]Firstly, one of the key aspects to assess is the "Accessibility and User-friendliness" of Government schemes through E-services. It is vital to determine whether the portals' layout makes it user-friendly to access the various features and services that are offered. The availability of thorough and current information is also essential. The efficacy of the e-governance portals would be compromised if citizens could not find the information they require or could not comprehend and use the platform. Second, it's important to assess how well the portals respond to and manage the needs of the public. The post-COVID-19 adjustments ought to prioritize expediting administrative procedures and cutting down on service delivery time. Enhancements in response times and the capacity to manage high request volumes would be signs of the e-governance portals' efficacy. It's critical to keep an eye on whether the portals have succeeded in lowering red tape and streamlining administrative processes. The evaluation of the post-COVID-19 modifications to Rajasthan's government schemes through E-services efficacy necessitates a comprehensive examination of several factors, such as technological integration, citizen participation, accessibility, responsiveness, and statistical data. After critically examining these variables, it will be plausible to pinpoint areas of strength, weakness, and potential for future development, which will ultimately result in more efficient and citizen-centric governance in the digital era. Statistical data and citizen feedback can be used to evaluate the success of post-COVID-19 modifications made to Rajasthan's Government schemes through E-services. Analyzing data such as user counts, services provided, and citizen satisfaction levels may bring insight into the effectiveness and impact of the modifications implemented. The government might analyze areas for development and increase the portals' efficacy by periodically conducting surveys with the public and getting their input.

II. METHODOLOGY

The researcher has collected 'data' from the survey done at the Krishi Vigyan Kendra in the Tonk district of Rajasthan. The researcher conducted empirical research and collected primary data by interviewing around 25 farmers in the Tonk district. The data was collected in physical form by circulating a questionnaire. Farmers shared their views honestly and with extreme sincerity. They not only told us the issues they face but also told us how the KVKs have done significant good to them by training them in making bio manure and bio fertilizers by creating a culture of decomposers, which is famously called *Apghatak* by them.

[1] Department of Information Technology and Communication, Government of Rajasthan, "E-Governance Initiatives in Rajasthan", *available at:* https://doitc.rajasthan.gov.in/ (last visited on March 28, 2024).

III. IMPORTANCE OF KVKS

Krishi Vigyan Kendras (KVKs) play a vital role in empowering farmers and advancing agricultural practices in India[2]. These are dedicated centers of government for facilitating "government schemes" toward farmers. These centers ensure that farmers have access to the latest agricultural techniques, knowledge, and resources to improve their productivity and overall income. One of the key aspects of a KVK's functioning is its regular recruitment drives, where vacancies are filled with individuals who are passionate about agriculture and are committed to serving the farming community. The recruitment process at Krishi Vigyan Kendra is rigorous and thorough, ensuring that only the most qualified and dedicated individuals are selected to join the team. These recruits are typically experts in various fields related to agriculture, such as agronomy, horticulture, soil science, and agricultural engineering. Their primary objective is to work closely with farmers, providing them with the necessary information, training, and resources to enhance their farming practices and overall output. These centers are equipped with facilities to conduct experiments and field trials to test new agricultural techniques and practices. By engaging in research and innovation, KVKs aim to develop sustainable solutions that address the challenges faced by farmers and help them adapt to changing environmental conditions.

Another crucial aspect of Krishi Vigyan Kendra's functioning is its proactive approach to engaging with farmers. These centres regularly host meetings, workshops, training programs, and field demonstrations to educate farmers about the latest agricultural practices and technologies, such as educating the farmers about the use of biofertilizers instead of urea and chemical fertilizers[3]. While having a word with the farmers, they all happily accepted that this step taken by the KVK has helped them reduce the expenditure they used to incur earlier. By keeping farmers informed and motivated, KVKs ensure that they remain associated with the center and continue to benefit from its services.

The timely call for meetings and events by Krishi Vigyan Kendra serves as a reminder to farmers to stay connected and engaged with the center. Through these interactions, farmers have the opportunity to exchange ideas, share experiences, and learn from experts in the field of agriculture. This collaborative approach fosters a sense of community among farmers and encourages them to adopt new practices that can lead to improved yield and profitability. These KVKs have a Sr. Scientist & Head and six scientists of different disciplines, including Agronomy, Horticulture, Plant Protection, Animal Science, Soil Science, and Home Science.

[2] S. Sulaiman and V.V. Hallie Eakin, "Agricultural Extension in India: Challenges and Opportunities" 47 *Economic and Political Weekly* 25 (2012).
[3] R. Saravanan, "ICTs for Agricultural Extension: Global Experiments, Innovations and Experiences" 48 *Indian Journal of Agricultural Economics* 379 (2013).

Well-equipped with technology, it calls for the position of Technical Assistant. Then various other posts for the role of Farm Manager, Programme Assistant Lab, Programme Assistant Computer, Accountant, Stenographer, 2 Supporting officers, and 2 Drivers.

It can be said that Krishi Vigyan Kendra plays a crucial role in supporting farmers and advancing agriculture in India[4]. Through their regular recruitment drives, focus on providing better facilities, and proactive engagement with farmers, these centres are helping to transform the agricultural landscape and empower farmers to achieve sustainable growth and prosperity. Therefore, the selection of K.V.K for the collection of the data was taken into account to carry out this research. The research required field visits and collection of data from the E-centres facilitating E-services. The centre chosen is K.V.K situated in the Tonk district of Rajasthan.

3.1. Farmers' Dependence on KVKs and E-Governance

Farmers do not make use of the e-portals directly, but are completely reliant upon the KVKs and other such institutional organisations[5]. Even though the aim of KVK, was to facilitate and equip the farmers to make them more tech-friendly who belong to the lower economic strata, unfortunately, it has not fulfilled the purpose, and therefore, such a lack of technical knowledge leaves them with no option but to depend upon the facilities like KVK for any sort of information[6]. However, the farmers were quite happy with the work of the KVKs. The importance of KVKs can't be denied as it initiates dispersion of the useful information to the farmers from time to time by calling them for the meeting and training them to make bio manures and decomposers at their homes and educating them about its benefits, with the least possible expenditure instead of expending huge amounts on Urea and Chemical fertilizers.

Farmers were timely given accurate weather information. This way, they are able to anticipate and prepare themselves beforehand, which in turn has reduced crop destruction to some extent. Farmers feel that it's the KVK that has helped them to correct a few ways of the farming techniques that have made the farming process a little easier. This has definitely raised the production to a certain extent. They are happy with the initiatives of the government to set up institutions like KVKs to educate farmers on the newer and more efficient techniques of farming.

[4] Indian Council of Agricultural Research, "Krishi Vigyan Kendras: Handbook of Agricultural Extension" 17 (2019).
[5] M.S. Swaminathan, "Reaching the Unreached: Information Technology and Agricultural Development in India" 37 *Economic and Political Weekly* 2347 (2002).
[6] Pippa Norris, "The Digital Divide: Civic Engagement, Information Poverty and the Internet Worldwide" 19 *Journal of Information Technology* 55 (2001).

IV. Market Value And Scale Of Finance: An Unfortunate Gap

With the increasing digitalization and technological advancements in India, the government has been striving to implement various e-governance schemes to benefit farmers across the country. These initiatives are aimed at improving the efficiency of agricultural practices, ensuring transparency, and providing timely access to information and services to farmers. However, despite these efforts, there remains a significant gap between market prices and the prices received by farmers for their produce or the SOF (Scale of Finance).

One of the key issues faced by farmers in India is the disparity between the prices they receive for their crops and the prices at which these crops are sold in the market. There are several reasons for this mismatch, such as a lack of price transparency, middlemen exploiting farmers, transportation costs, and market fluctuations. As a result, farmers often end up receiving lower prices for their produce, leading to financial losses and hardships.

Schemes introduced through e-governance by the government aim to address these challenges and empower farmers by providing them with access to real-time market information, price trends, and updates on government support programs. Platforms such as e-NAM (National Agriculture Market) have been established to facilitate online trading of agricultural produce and enable farmers to directly sell their crops to buyers across different states. Digital platforms such as the National Agriculture Market (e-NAM) have been developed to integrate agricultural markets and improve price discovery by enabling transparent online trading of agricultural commodities.[7] While e-NAM and other e-governance initiatives have made significant strides in promoting transparency and efficiency in agricultural markets, there are still several hurdles that need to be overcome to ensure that farmers receive fair prices for their produce. One of the key issues is the limited participation of farmers, especially smallholders, on online trading platforms due to factors such as a lack of awareness, internet connectivity, and digital literacy.

Moreover, the presence of intermediaries and traders in agricultural markets continues to pose a challenge to the effectiveness of e-governance schemes. Despite the government's efforts to eliminate middlemen and ensure direct farmer-to-buyer transactions, these practices persist in many parts of the country, leading to price manipulation and exploitation of farmers. To address these issues, there is a need for developing digital infrastructure and various initiatives like capacity-building programs and farmer training to enhance the participation of farmers in e-schemes. It is essential to empower farmers with the knowledge and

[7] Ministry of Agriculture and Farmers Welfare, "National Agriculture Market (e-NAM) Implementation Status Report" 21 (Government of India, 2021).

skills required to leverage digital platforms effectively and make informed decisions about marketing their produce.

4.1. The Scope of Crop Insurance Must Be Increased Through E-Services

Agriculture is the backbone of many economies around the world, providing food security and livelihoods for millions of people. Farmers face numerous challenges, including unpredictable weather patterns, pests and diseases, and market fluctuations[8]. These risks can have devastating consequences for farmers, leading to crop failures, financial losses, and even bankruptcy. To help protect farmers from these risks, insurance facilities for farm produce are essential. Insurance facilities for farmers offer a safety net against unforeseen events that can negatively impact their crops and livelihoods. These insurance products typically cover losses due to natural disasters such as droughts, floods, storms, and pest infestations, as well as market-related risks like price fluctuations and changes in demand. By providing financial compensation in the event of a loss, farm produce insurance helps farmers recover from setbacks and continue their operations. Insurance facilities with a wide horizon encourage farmers to adopt risk-mitigation strategies and invest in their farms, improving resilience and sustainability[9]. They also contribute to poverty reduction and food security by stabilizing farmers' incomes and ensuring continuity in agricultural production. This stability benefits consumers by providing a consistent and reliable food supply, even in the face of external threats.

4.2. Data Analysis: Technology And Educational Aspect

Farmers don't have the technical know-how or experience to take full advantage of e-governance programs. This can be the result of inadequate training on how to use digital resources for their agricultural requirements or restricted access to information and communication technologies. Because of this, farmers might not completely benefit from e-governance, which would affect their access to government programs, markets, information, and other necessities.

Through training programs and capacity-building activities, efforts should be made to improve farmers' technical abilities and digital literacy to address this issue. Enhancing farmers' participation with e-governance services can also be accomplished by offering straightforward interfaces and user-friendly platforms that are suited to their needs. Additionally, ensuring affordable and accessible digital infrastructure in rural areas is crucial to bridging the digital divide and empowering farmers to leverage digital tools for their benefit. By addressing these challenges and facilitating the meaningful participation of farmers in e-

[8] Richard Heeks, *Implementing and Managing eGovernment: An International Text* 23 (SAGE Publications, London, 2006).
[9]Subhash Bhatnagar, *Unlocking E-Government Potential: Concepts, Cases and Practical Insights* 45 (SAGE Publications, New Delhi, 2009).

governance processes, agricultural development can be enhanced, leading to improved livelihoods and sustainable agricultural practices[10].

4.3. Role of KVKS as the Facilitators and not the Sole Authority

The e-governance portals are primarily utilized by Krishi Vigyan Kendras (KVKs) and not directly by farmers. Consequently, farmers often rely on KVKs to access information and services available through these portals. Operations pointed out by you reveal the significant role of Krishi Vigyan Kendras (KVKs) in disseminating information and providing essential services to farmers. This dependence on KVKs showcases the crucial role they play in empowering and supporting farmers in adopting modern agricultural practices, accessing new technologies, and improving their overall productivity. This dependency on KVKs for bridging the gap between the portals and the farmers can be a crucial factor in ensuring the effective dissemination of knowledge and support to the agricultural community.

V. CROP STORAGE FACILITATION THROUGH E-PORTALS

"With almost 179.9 million hectares under cultivation, India has the second-largest amount of agricultural land in the whole world. In the context of global agriculture, the nation has become a significant factor[11]. Eleven percent of all exports from India are derived from agriculture, which contributes 14% of its GDP. India had an all-time high of 263.3 million tonnes (MT) of food grain output in FY 2013. The production of rice was 105.3 MT, while wheat production was 94.9 MT. Despite not having enough room to store it, the government purchases food grains from farmers".[12]

"There aren't enough covered godowns with enough storage space or grain silos—modern storage facilities—at the Food Corporation of India (FCI). Grain is therefore stored outside at CAP facilities around the country (Cover and Plinth). This makes grains more susceptible to pests, moisture, mice, and birds. The problem is made worse by the weather and unforeseen downpours. Every year, tons of food grains are lost due to inadequate infrastructure and storage. More fruit and vegetable waste occurs than with grains. Because of this, more financing is needed to establish suitable storage facilities for India's food supply system. Storage infrastructure is needed to preserve agricultural goods all year long and prevent distressed sales."[13]

[10]S. K. Sharma, "E-Governance in India: Challenges and Prospects" 45 *Indian Journal of Public Administration* 298 (1999).
[11] Iosr, J., Dr., B., & Lieutenant, C., "Agricultural Storage Infrastructure in India: An Overview" (2015), *available at*: https://doi.org/10.6084/M9.FIGSHARE.1424817.V1 (last visited on March 29, 2024)
[12] *Ibid*.
[13]A. K. Singh, "E-Governance and Agricultural Marketing Reforms in India" 54 *Indian Journal of Agricultural Economics* 321 (2019).

This problem is not new to the farmers of Tonk district. The researcher found this out when the farmers unanimously emphasized the issue of storage and how it is holding them back from making better profits for their produce. The issue is universal and has serious implications for the farmers as they spend a lot on the crop from the sowing of the seed till its harvest, and after harvesting, they have to face a significant loss when that crop gets destroyed because of a factor that could be mitigated by the government's intervention. It's not feasible for the farmers to spend huge amounts on the infrastructure for crop storage, which is why they have to witness rotting and spoilage of their agricultural produce. This issue must be further addressed with a proper database that would further help the farmers to locate such storage facilities near them, on their own, using the internet.

VII. Conclusion And Suggestions

The implementation of government schemes through e-services has revolutionized the governance model in Rajasthan, particularly in the post-COVID period. The research highlights the effectiveness of e-governance services in improving accessibility, user-friendliness, and responsiveness, which have positively impacted the residents of Rajasthan. However, the study also identifies the challenges faced by farmers, especially in terms of market prices and the SOF, which need to be addressed through better implementation and awareness of e-governance schemes. By focusing on these aspects, the government can ensure more efficient and citizen-centric governance, ultimately benefit the agricultural community and foster sustainable growth and prosperity.

Concerted efforts are needed to strengthen the regulatory framework governing agricultural markets and ensure compliance with fair trade practices. The enforcement of stringent laws and regulations to prevent price manipulation and unfair practices by middlemen will help create a more equitable and transparent trading system for farmers. Further, the issue of the non-availability of crop storage facilities must be done away with by establishing warehouses and storage, and a proper e-database must be set up for locating such facilities that must be extremely user-friendly and would not need much expertise to operate, as the farmers are not tech savvy. To further the ease of benefiting from the insurance, the facility of providing the 'necessary data' by the farmers should be provided through E portals to remove any hindrance and farmers can choose the insurance plan that best suits them with just several clicks. The facility for crop storage must also be included in the e-portals to truly reap the benefits of the new era of digitization of the agricultural sector.

1. Conduct awareness campaigns and training programs to educate farmers about e-governance schemes.
2. Improve infrastructure and connectivity in rural areas to ensure easy access to online platforms and services.

3. Promote direct farmer-to-consumer sales through online platforms to bridge the gap between market prices and the prices received by farmers.
4. Regularly conduct surveys and obtain citizen feedback to identify areas of improvement in e-governance services.
5. Enhance the transparency and efficiency of the agricultural supply chain by minimizing the role of intermediaries.

VIRAL SUICIDE GAMES: ONLINE PSYCHOLOGICAL MANIPULATION AND LEGAL GAPS

Aastha Gupta[*], *Dr. Neha Jain*[**] *and Asha Srivastava*[***]

ABSTRACT

The emergence of viral online "suicide challenges," such as the Blue Whale and Momo challenges, demonstrates how digital platforms can facilitate psychological manipulation and coercion of vulnerable adolescents. These challenges employ tactics including intimidation, gradual desensitization, emotional exploitation, and social contagion, often culminating in self-harm or suicide. While Indian legal frameworks address cybercrime, content moderation, and intermediary liability, they inadequately account for the psychological mechanisms through which such digital coercion operates. This article examines online suicide challenges as forms of cyber-enabled coercion and analyses the psychological processes that heighten adolescent susceptibility. Using qualitative content analysis of forty-six sources, including peer-reviewed journal articles, academic studies, policy documents, and reputable media reports, the study identifies recurring themes of adolescent vulnerability, coercive digital practices, social amplification, and regulatory gaps between law and psychological realities. The findings underscore the need for integrated platform safeguards, early mental-health interventions, and psychologically informed legal frameworks to proactively prevent digitally mediated coercion and self-harm among adolescents.

I. INTRODUCTION

The expansion of digital technologies has significantly changed the way people communicate and express themselves. In today's era, communication is primarily done through social interactions, which directly shape and determine how an individual constructs their identity as well as connect with other people in a social context. Researchers have highlighted that social media applications such as Facebook, Instagram, TikTok, and Twitter have changed the way of communication and relationships[1].

There has been an observable shift away from traditional human interaction and towards a greater online engagement as social media allows for quicker and easier

[*] The author is a Ph.D. Scholar at the Department of Psychology, The NorthCap University, Gurugram, and can be reached at aasthaoasis@gmail.com.
[**] The co-author is Head of Department & Associate Professor at the Department of Psychology, The NorthCap University, Gurugram, and can be reached at njain54@yahoo.com.
[***] The third co-author is Professor & Dean at the School of Behavioral Forensics, National Forensic Sciences University, Gandhinagar, and can be reached at ashacbi@gmail.com.
[1] I.M. Tarigan et al., "Understanding Social Media: Benefits of Social Media for Individuals" 23 *J. Pendidik. Tambusai* 2317 (2023).

communication between individuals. It has been observed that online engagement has escalated while the emotional connection and the depth of face-to-face relationships have declined[2]. The resources available for influencing decision-making have expanded significantly in the digital age, and in order to increase the sales of goods and services, people's digital footprints were initially analysed and recorded to obtain insights into their online habits. However, it has been seen that human behaviour is being influenced by digital technologies in ways that were not previously predicted[3] .There is now real-time access to ever-increasing amounts of individual-level data regarding granular aspects of people's online and offline behaviours[4]. This technical advancement has sparked public outrage in recent cases involving possible manipulation of online behaviour. Facebook records that were compromised revealed how advertisers could target adolescents online when they are feeling most vulnerable or insecure.[5]

These revelations raise important legal concerns regarding the responsibility of digital intermediaries when platform architectures and data-driven targeting practices expose adolescents to foreseeable psychological harm. While Indian cyber regulations primarily address issues of data protection, unlawful content, and intermediary compliance, they offer limited engagement with the legality of psychologically manipulative digital practices that exploit user vulnerability rather than merely disseminating prohibited content. This gap becomes particularly significant when such manipulation targets minors, who are recognised in law as a vulnerable class warranting heightened protection.

It has been highlighted that online manipulation challenges such as Blue Whale, Momo, Jonathan Galindo, and Skull Breaker that have gained popularity exploit human vulnerability, in various forms of online manipulation. Digital manipulation takes advantage of social influence and emotional exploitation; therefore, it is most likely to occur in digital environments where social cues distort easily and psychological triggers can be manipulated, thereby compromising the well-being and safety of individuals. Cyber grooming is the process of manipulating people digitally by targeting them (usually minors) and coercing them into becoming vulnerable, constituting an example of a digital risk-taking behaviour[6] . Digital spaces have become the venues through which

[2] E. Litt et al., "What Are Meaningful Social Interactions in Today's Media Landscape? A Cross-Cultural Survey" 6 *Social Media + Society* 1 (2020).
[3] S. Yu, "The Influence of Social Media on Interpersonal Relationships" 9 *Communications in Human Research* 90 (2023).
[4] S. Yu, "The Influence of Social Media on Interpersonal Relationships" 9 *Communications in Human Research* 90 (2023).
[5] Nitasha Tiku, "Get Ready for the Next Big Privacy Backlash Against Facebook", *Wired*, May 21, 2017, *available at*: https://www.wired.com/2017/05/welcome-next-phase-facebook-backlash/ (last visited on Jan. 25, 2026).
[6] M. Židová, "Cybergrooming as a Modern Form of Psychological Manipulation on the Internet" 14 *Slovak Journal of Education Sciences* (2024).

individuals can manipulate others psychologically, as evidenced by the increasing prevalence of viral online challenges. Viral "suicide challenges" are one of the most distressing psychological manipulations occurring online.

These challenges were predominantly circulated through social media platforms and private messaging applications, which consisted of a series of escalating tasks that encouraged participants to involve in self-harm and, ultimately, suicide. One of the earliest and most publicized examples of this is a suicide "game" called the Blue Whale Challenge which made an appearance on social networking sites like Facebook, Instagram, and Twitter in 2017. The fad appeared to have originated in Russia and subsequently spread throughout the world. Throughout the 50-day challenge, "players" were directed by "administrators" to perform daily tasks that involved progressively more harmful kinds of self-harm. The name of the challenge was derived from a disputed occurrence in which whales, highly sociable creatures that moved in herds, deviated from the group and beached themselves in a seemingly deliberate manner, resulting in their death.[7]

Similarly in 2018, youngsters also succumbed to another suicide game in addition to the Blue Whale Challenge. The Momo Challenge allegedly resembled its predecessor in many ways. The challenge involved teenagers interacting with the Momo WhatsApp account, which had an avatar of a hideous sculpture. When contacted, the Momo account posted graphic images and more difficult tasks that encouraged self-harm and suicide. Players who refused to do these tasks were known to have their accounts threatened with harm to their families or the revelation of confidential data[8]. Such practices indicate that these online 'challenges' function less as voluntary digital games and more as mechanisms of cyber-enabled coercion involving intimidation, psychological pressure, and threats.

The behaviours that have been highlighted are concerning from a legal standpoint in terms of the possibility of Criminal Intimidation and Abetment of Suicide as defined in the Indian Penal Code, particularly those behaviours whereby Psychological Pressure or fear induces Self-Harm without physically approaching someone. The methods of Psychological Manipulation and Influencing, including Cognitive Biases, Social Comparison and Emotional Contagion, play a very significant role in shaping Public Opinion, especially on social media. As such, understanding how and why these methods are being utilised on Social Media, both through the user interface and the way users perceive themselves, is critical

[7] Manish Upadhyaya & Marwan Kozman, "The Blue Whale Challenge, Social Media, Self-Harm, and Suicide Contagion" 24 *Primary Care Companion for CNS Disorders* (2022).
[8] "Man Gets Death Threat for Refusing to Play Momo Challenge in West Bengal", *New Indian Express*, Aug. 29, 2018, *available at*: https://www.newindianexpress.com/nation/2018/aug/28/man-gets-death-threat-for-refusing-to-play-momo-challenge-in-west-bengal-1864105.html (last visited on Jan. 25, 2026).

for users to protect their Mental Health[9].As highlighted in this article, despite the potential severity of these forms of harm, existing Legislation and Regulatory Frameworks in India continue to treat the phenomenon of Online Self-Harm mainly as it relates to Content Moderation and Intermediary Liability while ignoring the psychological Processes which exist behind Digital Manipulation, Compliance and Coercion. Moreover, this failure to understand the relationship between Digital Manipulation and Psychological Processes has significant ramifications for Digital Dignity and the Constitutional Right to Life pursuant to Article 21 as it relates to Adolescent Users operating in digitally-constructed and Algorithm-Driven Online Environments. Addressing the harms associated with Adolescent Self-Harm, therefore, necessitates an Interdisciplinary Approach which weaves Cyber Law and Civil Law Perspectives with Psychological Insights; thus, moving away from only addressing Content to embracing and understanding the psychological constructs associated with Coercion via Digital Means.

II. LITERATURE REVIEW

The rise of the digital age has led to many changes in the way individuals use technology and social media to control others. Psychological abuse is one type of digital manipulation and has become increasingly common. The increased access to the Internet and the speed at which information flows has given rise to new and previously unknown forms of victimisation, including covert or hidden online coercion and control. These forms of victimisation have long-term effects on an individual's mental health, sense of self, while instilling a sense of fear [10] .Offenders, through the use of digital technologies, can monitor, manipulate, and control others through emotional manipulation. The mechanisms behind this psychological abuse are associated with notions present in dark psychology, as well as trauma manipulation, and offer awareness into how victims are systematically monitored and manipulated, leading to serious disturbances. Survivors of online coercive control are particularly known to use thought control techniques, including rephrasing reality and stifling criticism.[11]

It has been highlighted in the research that, in addition to experiencing trauma symptoms similar to those of more conventional kinds of abuse, victims also feel abandoned, powerless, and betrayed by the system. These findings indicate that digital coercion operates through sustained psychological influence rather than isolated acts, requiring legal frameworks to recognise emotional and cognitive

[9] Sayak Pal, Susmita Halder & Nitesh Tripathi (eds.), *Psychology of Media Influence: Shaping Thoughts, Behavior and Society* (Mitra Press, 2025).
[10] The Constitution of India, art. 21.
[11] Molly Dragiewicz et al., "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms" 18 *Feminist Media Studies* 609 (2018).

harm as forms of legally relevant injury.[12] While digital coercion affects users across age groups, the majority of internet users are adolescents and young adults since they utilise it for socialising, completing schoolwork, and gathering information. Existing literature consistently identifies adolescents as the population who are in their developmental period marked by identity exploration, heightened sensitivity to peer evaluation, and incomplete maturation of cognitive control systems, all of which increase susceptibility to social influence and risk-taking.[13] According to contemporary research, individuals can be harassed, discriminated against, and socially disenfranchised via social media. It has also been noted that online communication, such as blogs, direct texting, and emails, has become essential to adolescents' social growth.[14]

Case reports from India and elsewhere show that curiosity, the desire for attention, loneliness, and pre-existing depressive symptoms commonly precede engagement with suicide-related challenges[15]. Empirical work linking problematic social media use to depression, anxiety, and stress in young people indicates that heavy or problematic engagement with online platforms is associated with poorer mental-health outcomes, which can in turn increase vulnerability to harmful online content[16]. Clinical notes throughout India and beyond indicate that before engaging in self-harm or suicide-related behaviours, many individuals report feelings of curiosity, needing to belong (i.e., social acceptance), loneliness, and pre-existing depressive disorders. From a legal perspective, this pattern of development makes the state constitutionally obligated to provide greater protection to minors under Articles 15(3), 21, and 39(f) of the Constitution of India. Collectively, this body of research has demonstrated how social learning processes within digital social networks propagate harmful behaviours, confirming what has been described as the Werther effect in suicide research; that is, the increased risk of imitation of a certain behaviour when exposed repeatedly to media news and sensationalistic reports of that behaviour through the Internet.[17] Online challenge formats convert social reward (likes, attention, peer recognition) into immediate reinforcement for risky acts, which promotes imitation and

[12] B. Pelz, "Trauma and Dark Psychology: Therapeutic Approaches to Manipulation, Control, and Power Abuse" 7 *Journal of Psychology & Neuroscience* 1 (2025).
[13] A.R. Bennett, *Digital Manipulation and Psychological Abuse: Exploring the Rise of Online Coercive Control* (Aug. 2025).
[14] H. Shannon et al., "Problematic Social Media Use in Adolescents and Young Adults: Systematic Review/Meta-Analysis," (2022).
[15] N. Fritz & A. Gonzales, "Privacy at the Margins—Not the Normal Trans Story: Negotiating Trans Narratives While Crowdfunding at the Margins" *International Journal of Communication* (2018).
[16] R. Narayan, "The Depressed Boy Who Accepted 'Blue Whale Challenge'" *Indian Journal of Psychiatry* 149 (2019).
[17] World Health Organization, *available at*: https://www.who.int/publications/i/item/9789240110069 (last visited on Jan. 25, 2026).

escalation. Moreover, the online disinhibition effect [18] reduces interpersonal inhibitions for both perpetrators and participants: perceived anonymity, distance, and asynchronous communication weaken empathic restraint and allow extreme suggestions and threats to be made with diminished accountability. When such social learning and disinhibition are embedded within platform architectures, the responsibility of digital intermediaries becomes central to the prevention of foreseeable psychological harm.

The blue whale challenge is one instance of self-harming behaviour that went viral and received a lot of media attention. According to the media, the game's developer, Russian psychologist Philipp Budeikin, intended to "cleanse the society of biological waste," which implies that those who are willing to commit suicide for the game are biological waste. This challenge consisted of 50 tasks that were assigned to adolescents, each of which had a higher degree of isolation and self-harm. Suicide and uploading evidence of successful completion were the last jobs assigned to the participants.[19] The Momo challenge was another popular cyber-suicide game in addition to the Blue Whale Challenge, which encouraged young children to commit acts of violence or even commit suicide. It was spread on messaging apps like WhatsApp and Facebook[20] . The images of the diabolical bird-lady appeared along with eerie directives and messages that escalated to severe violence and horror. According to some versions of the story, the horrifying image was included in YouTube videos of video games like Fortnite or children's shows like Peppa Pig.[21] These recurring patterns demonstrate that online suicide challenges function less as voluntary participation and more as digitally facilitated coercive systems involving intimidation, emotional pressure, and psychological dependence.

Adolescents (15–29 years old) are particularly vulnerable and susceptible to depictions of suicide and other forms of self-harm, and suicide is the second most common cause of death among this demographic[22]. The role of media is double-edged in amplifying reported instances of such online self-harming challenges. Both suicide prevention and suicide promotion were significantly influenced by

[18] John Suler, "The Online Disinhibition Effect" 7 *CyberPsychology & Behavior* 321 (2004), *available at*: https://johnsuler.com/article_pdfs/online_dis_effect.pdf (last visited on Jan. 25, 2026).
[19] R. Mukhra et al., "'Blue Whale Challenge': A Game or Crime?" 25 *Science and Engineering Ethics* 285 (2019).
[20] How the Facebook Feedback Loop Helped the Momo Hoax Go Viral, Wired, *available at:* https://www.wired.com/story/momo-challenge-facebook algorithm.(Last visited on Februrary 27, 2019)
[21] T. Lorenz, "The Bogus 'Momo Challenge' Internet Hoax, explained", *Vox, available at:* https://www.vox.com/2019/3/3/18248783/momo-challenge-hoax explained (last visited on March 3, 2019).
[22] L. Kobilke, "The Momo Challenge: Measuring the Extent to Which It Spread and Its Effects" 1 *SN Social Sciences* 641 (2021).

the media. The YouTube content[23] about the Momo Challenge was examined which depicted potentially harmful and helpful material. The Momo Challenge, like many previous social media challenges, was only an occasional trend. Suicide games, however, continue to expose teenagers to offensive video content and thoughts of self-harm, frighten children that scary characters like Momo might appear at night and harm them, and cause anxiety in parents[24]. In order to intimidate adolescents or obtain personal information, copycats may disseminate phone numbers and fictitious dialogues. On YouTube (or other short video applications), "where challenge videos have become an unusual trope of doing the most bizarre things to get views," the Momo Challenge is neither the first suicide game nor is it likely to be the last. Because many of these YouTubers target a younger audience that is unaware that these challenges are merely intended to garner views and likes, this trend is harmful[25]. The Jonathan Galindo Challenge and the Skull Breaker Challenge are two more suicide and self-harm games that were released in 2020, just two years after the Momo Challenge peaked. The Jonathan Galindo Challenge is the direct descendant of the Momo Challenge, whereas the Skull Breaker Challenge might be regarded as the Tide Pod Challenge's heir. These two self-harm challenges involve youngsters performing risky antics to make themselves appear trendy or humorous, such as kicking a third child's legs out from under him to knock him down or having them consume deadly detergent pods[26]. The increase of media amplification and algorithmic visibility escalate the harms already present in this medium and furthermore invokes the need to provide adequate regulatory oversight towards the distribution of user-created content by platforms.

The Information and Communication Technology (ICT) allows people around the world to communicate directly without intermediaries. Almost everyone now has access to the internet. The younger generations (youth) are the most affected by this technology because it affects every part of their lives and is inextricably tied to their lives. You can find almost anything or anyone in an infinite number of ways by simply searching with a digital device. These benefits of the digital world are accompanied by numerous hazards and challenges, and this is a common occurrence. Therefore, the evaluation, monitoring, and education of internet users, and specifically the youth, must begin immediately on matters related to internet

[23] A.B. Miller & M.J. Prinstein, "Adolescent Suicide as a Failure of Acute Stress-Response Systems" 15 *Annual Review of Clinical Psychology* 425 (2019).
[24] Supra Note 25.
[25] F. Lupariello et al., "Self-Harm Risk Among Adolescents and the Phenomenon of the 'Blue Whale Challenge': Case Series and Review of the Literature" 64 *Forensic Science* 638 (2019).
[26] E. Mazhari, "The Strange Story of How Tide Pod Eating Went Viral", *Forbes*, Feb. 5, 2018, *available at*: https://www.forbes.com (last visited on Feb. 5, 2018).

safety, security, and protection[27]. Under the Constitution, Article 21, the State's responsibility is to uphold the safety of individuals, both physically and psychologically [28], extends to the protection of their digital dignity in an increasingly virtual public domain. [29]

Recognising the growing acceptance that digital platforms have the potential for causing mental harm, the Government of India has provided numerous regulatory and service-level interventions to mitigate online abuse and enhance mental health support to at-risk groups. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, updated through 2023, require intermediaries to exercise due diligence, establish grievance redressal mechanisms, and remove unlawful or harmful content upon notification, measures directly relevant to moderating exploitative online game material30. More recently, the Promotion and Regulation of Online Gaming Bill, 2025, seeks to regulate online gaming platforms and explicitly recognises the need to protect vulnerable users from adverse psychological and financial harms while granting blocking powers for non-compliant services. [31]

These regulatory instruments reflect an evolving jurisprudential recognition that digital intermediaries are not passive conduits but active actors with corresponding duties of care toward vulnerable users[32]. At the same time, India's public-health response to mental-health and self-harm crises has gained new traction. The National Suicide Prevention Strategy (2022) provides a multisectoral roadmap for suicide prevention, calling for the reduction of suicide mortality by 10% by 2030 33. Complementing this, the National Tele-Mental Health Programme (Tele-MANAS), launched under the MoHFW, has established 24×7 helpline services offering tele-counselling and psychological support across states (MoHFW, 2024). These initiatives demonstrate the State's preventive and rehabilitative obligations under Articles 15(3) and 39(f) of the Constitution to protect children and adolescents from psychological and moral harm. On the other hand, Bharatiya Nyaya Sanhita, 2023, has modernised criminal law frameworks

[27] A.R. Ram & T.R. Subhikshan, "Safeguarding Children in the Digital Age: Legal Challenges and Strategic Responses to Online Exploitation" 7 *International Journal of Legal Science and Innovation* (2025).
[28] O.P. Singh, "Use of Digital Media in Suicide Prevention in Adolescents and Young Adults" 61 *Indian Journal of Psychiatry* 1 (2019).
[29] J. Srivastava, V. Srivastava & P. Rai, "Cyber Safety of Students in India and China: A Comparative Analysis of Policies and Practices" *YMER* (Nov. 8, 2024).
[30]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated 2023), *available at*: https://www.meity.gov.in (last visited on Jan. 25, 2026).
[31]Promotion and Regulation of Online Gaming Bill, 2025, Bill No. 110 of 2025.
[32]Press Information Bureau, "Promotion and Regulation of Online Gaming Bill, 2025 — Parliamentary Update", Aug. 21, 2025, *available at:* https://pib.gov.in (last visited on Jan. 25, 2026).
[33]Ministry of Health & Family Welfare, "National Suicide Prevention Strategy" (2022).

of India. Nonetheless, its provisions on cyber offences related to the psychological manipulations present in online games are not directly linked to the abetment of suicide[34]. Although Section 108 of the Bharatiya Nyaya Sanhita[35] criminalises abetment of suicide, its application to digitally mediated coercion remains legally underdeveloped, particularly where instigation occurs through sustained psychological pressure rather than direct incitement. This legislative gap underscores the continuing disconnect between criminal liability doctrines and the complex psychological realities of online manipulation.

III. METHODOLOGY

This study employed a qualitative content analysis methodology on forty-six (46) sources to examine the psychological and social processes surrounding online suicide challenges, with specific reference to the Blue Whale and Momo challenges. The study relied on secondary resources, which are publicly available such as peer-reviewed empirical and qualitative research articles, policy documents, and reputable media reports concerning digital manipulation, self-harm, and online behaviour of adolescents. The objective of the study was to investigate the structural mechanism of online suicide challenges, the manipulation tactics employed, and the emotional vulnerabilities of victims. The data was analysed as well as coded using the six-step thematic analysis framework developed by Braun and Clarke, which comprised the following steps: 1) becoming familiar with the data, 2) generation of initial codes, 3) theme development, 4) reviewing of themes, 5) defining and naming of themes, 6) creating a systematic report of the results. The coding and thematic interpretation were conducted manually to maintain close engagement with the data and analytical consistency. Since the study was exclusively based on secondary data, ethical considerations were observed by relying solely on publicly available, anonymised, and verifiable sources, thereby ensuring compliance with established research ethics standards.

IV. RESULTS

The researchers employed quantitative content analysis to study repeated patterns from the way that psychological, clinical, media, and legal resources related to suicide challenges pervade the Internet, finding several distinct themes associated with the ways that digital manipulation occurs, how vulnerable adolescents were exploited, and weaknesses in regulatory frameworks. The four themes were constructed by analysing the similarities, overlaps, and relational patterns among sub-themes to create a higher-level conceptual grouping of themes. Table 1

[34]PRS Legislative Research, "The Bharatiya Nyaya Sanhita, 2023" (2023), *available at:* https://prsindia.org (last visited on Jan. 5, 2026).
[35]The Bharatiya Nyaya Sanhita, 2023, s. 108.

presents the condensed listings of each of the four major themes, their operational definitions, and examples of sub-themes.

Table 1: Key Themes, Operational Definitions, and Illustrative Sub-themes

Key Theme	Definitions	Example subthemes
Adolescent Vulnerability and Emotional Susceptibility	Developmental, emotional, and cognitive characteristics that increase adolescents' susceptibility to digital manipulation and self-harm-related influence	Emotional reactivity, identity confusion, peer sensitivity, loneliness, depressive symptoms, belonging-seeking behaviour.[36]
Coercive Digital Practices, Gradual Desensitisation, and Compliance	Systematic psychological strategies used to induce dependency, reduce resistance, and secure compliance through escalating online tasks	Task escalation, emotional threats, isolation, fear of exposure, psychological dependence[37], proof-sharing, grooming practices.[38]
Social Contagion, Platform Dynamics, and Media Amplification	Processes through which harmful behaviours spread and are reinforced through peer validation, media coverage, and algorithmic visibility	Behavioural modelling, viral sharing, moral panic, imitation, social rewards[39], algorithmic promotion.[40]
Legal–Psychological Disconnect and Policy Implications	Mismatch between regulatory approaches and the psychological mechanisms underlying digital manipulation and self-harm	Content-focused regulation, limited preventive safeguards, inadequate mental-health integration, weak psychological recognition in law.[41]

[36]T. Joiner et al., "Main Predictions of the Interpersonal-Psychological Theory of Suicidal Behavior: Empirical Tests in Two Samples of Young Adults" 118 *Journal of Abnormal Psychology* 634 (2009).
[37]A. Khasawneh et al., "Examining the Self-Harm and Suicide Contagion Effects of the Blue Whale Challenge on YouTube and Twitter: Qualitative Study," (2020) 7 *JMIR Ment. Health* e15973.
[38]Supra note 37.
[39]A. Bandura, *Social Learning Theory* (Prentice-Hall, 1977).
[40]G. Ramkumar & V. Singh, "It Is a Rumour-Panic: A Sociopsychological Case-Study of the Media-Spread of the 'Blue Whale' Suicide Game and the Responses to It in India" 35 *Indian Journal of Social Psychiatry* 250 (2019).
[41]Y.P.S. Balhara et al., "The 'Blue Whale Challenge'?: First Report of a Consultation from a Health-Care Setting for Carrying Out Tasks Accessed Through a Mobile Phone Application" 10 *Asia-Pacific Psychiatry* (2018).

V. DISCUSSION

The present study examined the psychological, social, and legal dimensions of online suicide challenges through a qualitative content analysis of secondary sources. The findings reveal that such challenges are structured systems of manipulation that exploit vulnerability, platform dynamics, and regulatory gaps. By integrating psychological theory with legal analysis, this study contributes to a more comprehensive understanding of how digitally mediated coercion operates within contemporary online environments.

5.1. Theme 1: Adolescent Vulnerability and Emotional Susceptibility:

The first major theme highlights that adolescents and young adults were over-represented in the sources that addressed viral suicide challenges. Many sources remind us that this period of development is characterised by intense emotional reactivity, a slowly developing sense of self, and an intense awareness of popular opinion. Research relating to the Blue Whale Challenge found that those involved were often individuals with pre-existing depressive symptoms, feelings of loneliness or isolation, as well as tendencies toward self-harm. The initial tasks in the challenge sought to increase participants' physical pain tolerances while simultaneously reducing fear of death. This increase in pain tolerance and insouciance toward death is related to elements of the interpersonal-psychological theory of suicide. These findings indicate that the manipulators are purposefully exploiting the vulnerabilities that characterise adolescence, underdeveloped cognitive control, emotional instability, susceptibility to public opinion, and the desire to belong. Thus, children and adolescents become the primary targets of these digitally coercive phenomena. The challenges are designed to create a sense of belonging (for instance, "you are part of a special group") while also slowly, incrementally increasing the risks, thus granting adolescents the benefits of a perceived sense of self and purpose, while guiding them toward self-harm. This duality of a commonality of the connecting dynamic while under subtle manipulation works powerfully in online environments, particularly where parental or institutional supervision is weak.

5.2. Theme 2: Coercive Digital Practices, Gradual Desensitisation and Compliance

The second theme that emerges from the sources is the nature of these challenges: a series of progressively more demanding tasks which gradually desensitise the participants, create psychological dependence, and ultimately lead to suicide or cause severe self-harm. The Blue Whale Challenge reportedly consisted of around fifty tasks that consisted principally of innocuous tasks (waking at 4.20 a.m., watching horror films) and went on to cutting, self-harming, isolation, and finally suicidal behaviour. The thematic analysis of YouTube and Twitter data similarly found that many of the videos were contravening the guidelines for safe messaging and thus creating the risk of the normalisation of self-harm.

From the psychological aspect, the nature of the design mirrors that of coercive behaviours and gradual desensitisation: the person is first gradually led into the scheme by being given small tasks, is then altered subtly through emotional control (threats, isolation, fear of exposure), the tasks are made more serious and by the time a withdrawal would happen, the control is held by the manipulator—in the form of social, emotional and occasionally digital control (threats to expose personal data). The online medium amplifies these needs: anonymity of the curator, 24/7 availability of tasks, algorithmic spreading of peer-validated footage or "proof" videos, and platform affordances that make withdrawal difficult or shame-inducing. The overall effect means that participants are often favoured with emotions of entrapment, helplessness, and deepening personal investment in psychological terms, which has been the end state sought by the manipulator.

5.3. Theme 3: Social Contagion, Platform Dynamics, and Media Amplification

The third theme highlights the viral nature of these challenges and their means of amplification through their circulation in social media, messaging applications, and mainstream news media. Social learning theory helps explain how adolescents may imitate behaviours when they see them rewarded (by likes and shares) or socially approved (through acquiring social status). For instance, with the Blue Whale Challenge, many YouTube posts and social media were discovered with comments that normalized participation by sharing stories or videos, positing a risk of behavioural contagion through modelling. Similarly, the study in India, "It's a Rumour-Panic: A Sociopsychological Case Study of the Media-Spread of the 'Blue Whale' Suicide Game," argues that the media coverage frequently fostered a moral panic and fear rather than increasing properly informed awareness. Media reports were sometimes responsible for magnifying the Challenge, even attributing to it suicides without verification.

This magnification produces a self-perpetuating cycle: awareness produces curiosity, curiosity increases imitation, and imitation produces harm. Moreover, the features of the platforms used, such as algorithmic visibility and the instant circulation afforded by messaging applications, further reduce barriers to the dissemination of these content forms, increasing the degree of the latter's reach in a way that offline, manipulatively occurring contexts can never achieve. To prevent manipulation of this nature, it is important to understand the larger framework that supports this activity, as well as the fact that prevention needs to target both individuals and the larger structural, social, and technological processes that allow for this harm.

5.4. Theme 4: Legal, Psychological Disconnect and Implications for Policy

The fourth theme establishes a profound disconnect between the legal response to manipulation and the psychological factors associated with it. The Indian legal framework, the IT (Intermediary Guidelines & Digital Media Ethics Code) Rules,

2021, and the Promotion of Online Gaming and its Regulation Bill, 2025, represent very important steps forward. The qualitative thematic analysis also indicates that these regulations focus on two areas of content moderation, platform responsibility, and the need for mental health services, with inadequate attention to the subtle psychological mechanisms that operate in coercive grooming, desensitisation, and mimicry. Such a discrepancy may adversely affect the effectiveness of preventive measures, e.g., laws concerning "games" that do not act on the underlying emotional manipulation do not influence the coercive process.

From a mental health perspective, case studies emphasize the importance of early recognition of adolescents who have curiosity about or engagement in online challenges. However, many institutions still lack any structured form of configuration to assess and respond to the risks associated with digital coercion. These findings highlight the importance of a holistic approach to preventive measures: legal regulation, platform development, advocacy and awareness amongst parents and educators, and mental health screening must all be informed by evidence of the underlying psychology. In conclusion, the online manipulative suicide challenges gain by exploiting the vulnerabilities of youth, the affordances of the digital platforms, and the rapidity of dissemination, where existing safeguards are incomplete. The article recommends that, by bringing together the psychological, social, and regulatory perspectives, more than the regulation of content needs to take place, an understanding of the nature of how manipulation occurs and how it can be attacked.

VI. Implications And Suggestions

The present study offers several actionable insights for policymakers, digital platform administrators, educators, mental health professionals, parents, and researchers concerned with the prevention of online suicide challenges and digitally mediated psychological harm. These findings indicate a direct need for the development of interventions for all age groups that are proactive and offer psychological information to support this population. Further, the digital platform's design must include the development of intervention strategies and ways to prevent the use of digital coercion such as by creating a "roadmap" for intervention strategies. Digital platforms offering user-generated content should include safety measures available through predictive algorithms to indicate when an increase in risky participation is noted in an individual's use of the platform. Digital platforms should have trained legal moderators, parents, or child protection agencies on standby to monitor for those who may be at risk of self-harm or social withdrawal, and to offer intervention assistance to those at risk. It is important that digital platforms also ensure the safety of their users' ages, and to eliminate users' ability to post anonymously in situations where there is a compelling danger to another person. In addition to the combination of digital

safety intervention strategies for adolescents, it is equally important to have a mental health prevention program in place to create resiliency in adolescent populations. A mental health prevention program would also include a focus on early recognition through training on warning signs of potential self-harm, as well as an awareness of a youth's active involvement in secretive tasks, and the reliance on social support through virtual means. Mental health screening of adolescents followed by intensive counselling through school systems would provide the opportunity for early identification of youth needing mental health support, allowing for the development of supportive structures to meet their needs prior to engaging in potentially dangerous behaviours.

The study also highlights the need for new legislative and regulatory frameworks for how society decides to regulate what constitutes acceptable interaction between end-users (i.e., parents/adults) and digital game providers. As users are perpetually faced with coercive forms of interactions on both social media and gaming platforms, a carefully created legal infrastructure outlining acceptable norms will be critical for policymakers to provide as a basis for regulating these interactions and relationships. The study will also guide future policy creation regarding collaboration between institutions that support youth dealing with potential self-injury as a result of coercive interactions online and collaborative partners/participants implementing short- and long-term interventions to reduce and assist in the prevention and treatment of and for victims of cyber bullying. This study also illustrates the need for continued longitudinal and interdisciplinary research regarding the relationship between coercive behaviours online and the psychological effects of these coercive behaviours on victims over time, as well as the effectiveness of preventative interventions. It is also important for teacher, police officer, health professional, and online forum moderator training programs to incorporate data and research that have been validated to aid in understanding the influence of coercive online behaviours upon youth, their mental growth, and their psychological resiliency. By working proactively to mitigate the risks for adolescents in digital spaces, instead of reacting retrospectively to crises after the fact, all stakeholders can create safer environments for adolescent users and, therefore, will support a premium on the healthy social, emotional, and psychological development of adolescents and their combination of autonomy and the development of psychological resiliency.

VII. Limitations And Directions Of The Future Research

This study is based on secondary sources and publicly available materials, which may limit access to first-hand experiences of affected individuals. The findings therefore depend on the accuracy and completeness of existing reports and publications. Additionally, the qualitative nature of the analysis does not allow for statistical generalisation of results. Future research may benefit from primary data collection, including interviews and surveys, to gain deeper insights into the

lived experiences of victims and the effectiveness of preventive intervention. Moreover, new laws should be made and existing laws should be made stricter to hold perpetrators accountable and safeguard against recruitment through platforms such as email or messaging apps. Multi agency integrating cybercrime units, mental health services and educational institutions should make coordinated efforts in strengthening and implementing timely interventions for at-risk youth and make sure that they receive the protection and support required.

CYBERSECURITY AWARENESS AND CAPACITY BUILDING IN INDIA: A GRASSROOTS APPROACH

Pakhi Kansal*

ABSTRACT

The onset of a digitally connected life in India has ushered in a new way of performing and facilitating economic activity, financial services, education, and governance as a whole. Although it is in tandem with other advances, the extent and complexity of cyber threats have dramatically increased. While initiatives like Digital India, BharatNet, and Smart Cities Mission are pushing the nation forward at a rapid pace and incorporating and involving such large segments of society in cyberspace as never before, it must not be overlooked that such large segments of society are joining cyberspace without understanding cyber threats and best practices in cyberspace behaviour and activity. Therefore, there are dual pressures in India: securing critical cyber and information infrastructure and, at the same time, encouraging responsible and safe behaviour in cyberspace among its citizenry.

This article delves into the need for a comprehensive approach towards cybersecurity in the Indian context. The matter is addressed through a critical evaluation of the mismatch between nationwide cybersecurity policies and their implementation in practice, particularly in non-urban sectors where digital education is still in its nascent stage. While the policies, such as the National Cyber Security Policy of 2013, primarily relied on preparedness within institutions and security measures within institutions, very little focus has been on mass-scale engagement. The National Cybersecurity Strategy in 2024 is a much-needed turning point where the focus needs to shift towards mass development.

The article incorporates a study that also considers the potential use of programs intended to enhance cyber hygiene skills through workshop training programs, awareness activities, and online training offered at the national or state administration level. Additionally, the role played by higher educational institutions, business organizations, and other civil society groups is considered. Designing cybersecurity education inclusive, multilingual, and responsive to socio-cultural settings is discussed at length. Raising basic awareness about cybersecurity among panchayats, self-help groups, and school teachers is identified as an important initiative to improve the overall cybersecurity system in India.

* The author is an LL.M. student at the K. R. Mangalam University, Sohna, Haryana, and may be reached at pakhikansal0707@gmail.com.

I. INTRODUCTION

The digital revolution in India has transformed the ways of communication, education, banking, business, and governance. The Indian Government, through initiatives such as BharatNet, Digital India, and Smart Cities Mission, has provided digital access to millions of citizens in both rural and urban settings. The Government of India, through initiatives such as BharatNet, Digital India, and the Smart Cities Mission, has provided digital access to millions of citizens in both rural and urban areas. This has paved the way for new opportunities for social inclusion, innovation, and economic participation. However, this has made the citizens of India, by and large, vulnerable to cyber threats. The fact is that with an increase in usage of digital services, the users of digital services face threats of cyber fraud, identity theft, and cybersecurity breaches owing to their relative lack of knowledge and awareness, especially among first-timers in rural and semi-urban areas. Cybersecurity has, therefore, suddenly entered the realms of public trust and national security, rather than remaining confined to purely technical domains. India needs to ensure its citizens not only remain connected but also utilize technology sensibly and safely in order to preserve their digital advances in this respect.[1]

While the information technology policies of India, such as the National Cyber Security Policy in 2013, recognize the need for the resilience of the country's infrastructures and the shielding of the institutions of the country from cyber threats, they tend to negate the importance of grassroots levels of community empowerment in the field of cyber threats.[2] Rather than a mere focus on the infrastructures of the country and the safeguarding of the nation's institutions in the context of cyber threats and their prevention, the need for the development of a cyber-aware citizenry in a country such as India cannot be overestimated in terms of the country's evolving information and digital revolution. Thus, the need for the creation of an educated, watchful, and cyber-aware citizenry in India in connection with the evolving digital revolution is as great as the need for any additional India-specific technological advancements in the field of cyber protection.[3]

II. RESEARCH PROBLEM

There is clearly a wide gap formed between the planning and actual implementation at the grassroots level, even in stronger frameworks such as the National Cyber Security Policy (2013) and the efforts made by organizations such

[1] Ministry of Electronics and Information Technology (MeitY), Digital India Programme, Government of India, 2015.
[2] NASSCOM–DSCI, Cyber Security in India: Policy, Strategy and Implementation (New Delhi: NASSCOM, 2020).
[3] World Bank Report, Digital Development in South Asia: Challenges and Opportunities, Washington D.C., 2022.

as CERT-In and NCIIPC. With little reach extended to the rural and semi-urban population, which constitutes an important part of the significant number of new users on digital platforms, the strategies remain largely institutional and urban-oriented. With the population at large threatened by internet fraud, misinformation, and data abuse because of the lack of appropriate grassroots and culture-specific, language-friendly, and conscious cybersecurity knowledge, it is essentially the approach adopted by this research challenge, which is primarily centered on awareness and capacity-building mechanisms as to how the national strategies on cybersecurity can be extended to the grassroots levels.[4]

III. Objectives Of The Study

The study seeks to explore the requirements and efficacy of the community-based model for cybersecurity in India. Specific objectives of the study are:

1. To understand the level of cybersecurity awareness in the rural and semi-urban population.
2. To explore gaps that exist between national cybersecurity policy and implementation on the grassroots level.
3. The impact of government bodies, the academe, the corporate sector, and the civic sector in the promotion of digital literacy and cyber hygiene practices.
4. To present a framework to build capacity regarding localized, multilingual, and inclusive cybersecurity.

IV. Research Methodology

In order to analyze and gain insight into the dual nature of cybersecurity awareness and capacity building, this study uses an integrated research approach in which empirical research is complemented with interpretation. The use of an integrated methodological design in this research work serves as an impetus for this study to dive deeper into community-level experiences related to cybersecurity challenges and to gain an understanding of this crucial issue. Empirical Assessment through Quantitative Tools:

The quantitative part of the research works on the premise that structured survey research tools and questionnaires are being conducted and fielded in rural and semi-urban areas to reflect grassroots awareness and familiarity regarding cyber safety and awareness. These research instruments are being used to understand the degree to which people are exposed to and aware of cyber safety practices, and familiarity and awareness regarding basic digital knowledge and internet usage. The results that emerge from such research data are analysed and processed to identify trends and linkages regarding grassroots awareness and familiarity

[4] Ankit Kumar et al. "Cybersecurity Awareness and Digital Literacy in the Context of Digital India" 11(4) *International Journal of Applied Research* 434–439 (2025).

levels and corresponding demographics such as age, education, profession, and use of the internet, among others. Cyber safety awareness is evaluated based on research variables that include familiarity and awareness regarding phishing, password protection, online fraud, and grassroots awareness regarding cyber scams, among others.[5]

Contextual Inquiry through Qualitative Exploration:

In order to add to the quantitative results, the article introduces a qualitative component that involves the conduct of semi-structured interviews and group interactions. It includes the following as the target participants: teachers in local schools, government officials, personnel responsible for the training of cybersecurity, and officials from civic societies. The expected outcome of the qualitative research helps in providing a clearer understanding of the influencing factors of social, cultural, and behavioral aspects, as far as digital practices and cybersecurity in rural as well as semi-urban areas are considered.

Evaluation of Policy Frameworks and Comparative Perspectives: Besides the primary research, there is also an analysis of the pre-existing policies and capacity-building efforts made at the national and state levels to combat the issue of cybersecurity. This analysis has been carried out with the objective of determining the effectiveness, availability, and reach of these efforts at the community level.[6] Alongside, there is also a comparison of the community-based models of cybersecurity implemented in other developed nations, such as Singapore and Estonia, by which the researchers can obtain the best-practice strategies and implement them as per the needs of the Indian environment. Through the descriptive and analytical methodology, the study outlines the challenges associated with global digital literacy and cyber vulnerability.

V. Cyber Threats And Vulnerabilities In A Digitally Expanding Nation: Case Studies And Risk Analysis

India has emerged as one of the world's largest online marketplaces due to the rapid evolution of its digital space, but this has also made people and organizations more susceptible to attacks. This rapid transition to a digital economy has exposed India to increased cyberattack risk due to the extensive use of online transactions, digital governance, and connected devices. Apart from large companies and government bodies, the current major types of cyber-attacks, such as phishing, ransomware attacks, malware attacks, data breaches, and social engineering attacks, also now threaten small companies and civilians. One such attack took

[5] Anupreet Kaur Mokha "A Study on Awareness of Cyber Crime and Security" 8 *Res. J. Human. & Soc. Sci*. 459 (2017).
[6] Madhuri Paradesi "Cybersecurity Laws in India and Beyond: A Comparative Analysis" 12 *Int'l J. Mech. & Human.* 1734 (2021)

place in the Cosmos Bank in 2018[7], wherein attackers infected the bank's computer system with malware and in mere hours, removed nearly 94 crores via global transactions. Similarly, the Kudankulam Nuclear Power Plant[8] in India faced a possible attack from malware in the year 2020, resulting in the vulnerability to attacks on the critical infrastructure of India.[9]

Government databases are now an attractive target for hackers due to the increasing digitization of public services and governance. The 2018 breach of Aadhaar data[10] reportedly exposed private biometric and demographic data of millions of users which highlighted the risks of centralized data repositories. The 2021 Air India[11] data breach exposed personal information of over 4.5 million passengers and involved impacts concerning Indian and foreign stakeholders. The 2022 AIIMS ransomware attack[12] demonstrated the severe consequences of cyber-attacks against critical healthcare infrastructure by disrupting the functioning of hospitals for several days. Educational institutions and e-learning platforms have seen increased attempts at phishing and defacement, especially during the COVID-19 pandemic when online learning became routine. The education sector has not remained far behind either. Additionally, , cybercrimes that exploit the rapid adoption of digital payments without corresponding benefits in awareness, such as phishing messages purporting to be government entities, fake loan app scams, and UPI payment frauds, are some common instances that have gained more traction amongst the rural and urban population.

The security challenges in India are inextricably interlinked with their socioeconomic diversity, disparity, and lack of uniform cybersecurity awareness; thus, there's a comprehensive risk assessment of such cases. While there has been an improvement in terms of screening and responding efforts by organizations such as CERT-In and NCIIPC, most citizens are unaware of the basic cybersecurity best practices. While community-level awareness efforts in grassroots settings, such as Telangana's Cyber Warriors and Kerala's Digital

[7] Dhaarani S. & Aaliya Ameer A. "A Case Study on Cyber Security Threat to Cosmos Bank" *3 Indian J. Integrated Res. L.* 505 (2023).
[8] Maj. Gen. P. K. Mallick, Cyber Attack on Kudankulam Nuclear Power Plant: A Wake Up Call (Vivekananda Int'l Found. Dec. 18, 2019)
[9] Reserve Bank of India, Cyber Security Framework in Banks, Circular DBS.CO.CFMC.BC.No.2/23.04.001/2016-17 (June 2, 2016).
[10] Brett Orren "India's Data Wild West: The Aadhaar System and Its Questionable Data Protections" 45 *N.C. J. Int'l L.* 619 (2020)
[11] Evert De Clercq, Data Breaches and Airlines: Lessons Learned! (BARIN Nov. 2021)
[12] Vinod Kumar Mishra & Shilpi Khandelwal "Cyber Security Challenges in Indian Corporations in View of Recent AIIMS Server Hack" 5 *Int'l J. Commc'n & Info. Tech*. 33 (2024)

Literacy Mission[13], have resulted in significant mitigation of risks, it has not yet been adopted at a national level.[14] The linguistic and cultural diversity in India requires that respective regions need to be addressed differently and in conjunction with technology protection. Thus, to build a strong cybersecurity framework, it has to be addressed with a dual approach—incentivizing development in cybersecurity infrastructure, and putting communities, too, in the initial defense position against cybersecurity risks. For India to reduce, the rising number of cybersecurity threats accompanying their technological development, it needs to adopt an inclusive and comprehensive strategy.[15]

VI. Policy Frameworks And Institutional Mechanisms – Review Of NCPS (2013), CERT-In, NCIIPC, And Upcoming Policy Developments

There exists a multi-layered institutional and policymaking framework that helps to safeguard 'digital infrastructure' and prepare a joint response to the 'cyber threat' challenges. This serves as a basis for the management of the Indian 'cybersecurity' framework. The key policymaking document, which encapsulates 'strategic' objectives such as the 'protection of information security,' the development of 'cyber human resource talent,' as well as 'public-private partnership' building activities, remains the 'National Cyber Security Policy (NCSP) Statement' of 2013.[16] It fundamentally focuses on the 'cyber resilience' of citizens and companies through 'incident response,' 'capacity building,' and 'legislated measures'. Nevertheless, this 'policy response' of the Indian state has been grossly 'criticized' as 'outdated' and 'unripe' in its 'action-oriented imperatives' as far as 'ransomware' as well as 'data breaches' are concerned. Therefore, the 'Indian state' recently 'launched' the 'National Cybersecurity Strategy (NCSS) 2023 having the 'look-and-feel' of 'introducing state-of-the-art technology such as 5G, cloud, AI into a 'safe' 'cyber ecosystem' as its 'foundation stone' aimed at improving the 'cyber resilience' of the 'energy, finance, and hospitals sectors,' 'data localization' within India, as well as making 'institutional collaboration' among a few 'Indian Ministries' even 'stronger' than before.[17]

[13] Electronics and Communications Department Annual Report, 2021-22*, available at:* https://invest.telangana.gov.in/wp-content/uploads/2022/06/Telangana-IT-EC-Department-Annual-Report-2021-22.pdf (last visited on May 20, 2026)

[14] CERT-In, Annual Report 2023-24, Indian Computer Emergency Response Team, Government of India.

[15] National Crime Records Bureau, Cyber Crime in India: Statistics 2023, Ministry of Home Affairs, Government of India.

[16] MeitY, National Cyber Security Strategy (Draft), 2023, Government of India.

[17] Priyanka T. Sawale "Cybersecurity Awareness and Digital Safety Practices Among Secondary School Teachers in Urban and Rural Areas of Nashik" 5(2) *Journal of Informatics Education and Research* (2025).

To a large extent, institutional structures like NCIIPC and CERT-In operationalize the country's cybersecurity strategy. As the national nodal agency, CERTIn is responsible for responding to emergencies, sending out security warnings, and helping public and commercial organisations coordinate their efforts in response to cyber incidents. It has proved quite efficient in mitigating the impact of widespread attacks, such as ransomware threats, malware outbreaks, and phishing. On the other hand, NCIIPC, established under NTRO, is mandated with the duty of protecting essential infrastructure, comprising defence networks, banking systems, telecommunications, and power grids.

VII. Grassroots Realities: Awareness, Access, And Challenges – Field Data, Surveys, And Observations

Though there has been rapid digital growth in India, a large number of citizens, especially in rural and semi-urban zones, have remained digitally marginalized because of a lack of awareness, infrastructural bottlenecks, and socio/economic factors. The surveys undertaken by NASSCOM -DSCI in 2022, conducted in 15 districts in Uttar Pradesh, Bihar, and Odisha, have shown that more than 60% of rural internet users have never undergone any formal training on online security etiquette. Though consumers show eagerness for digital adoption, such as e-banking and government websites, the vast majority lack familiarity with basic components of online security, such as using secure passwords, phishing, or secure digital payment systems, as observed during field visits with self-help group members and staffer members in panchayat offices.

Further ground research in the Telangana region of India and the state of Kerala has evidenced the effectiveness of community-led intervention programs in improving the general public's cyber awareness. Telangana's pilot research of a group of 200 families in the country's rural areas found a reported enhancement of 45 per cent in cyber awareness of the participants of the 'Cyber Warrior' project[18] against the control group in a phishing and cyber fraud awareness context. Similarly, in Kerala's Digital Literacy Mission[19], a focus group discussion among participants indicated that hands-on training for teachers and community leaders improved the effectiveness of disseminating cyber awareness in villages. . Yet the effects are still constrained by erratic internet connectivity, the availability of reasonably priced equipment, and the digital literacy levels of the teaching community in the region. According to a survey of the Digital India initiative of the group, over-reliance on unofficial cyber networks and

[18] Gov't of Telangana, Telangana Cyber Security Policy (2016)

[19] Anandraj K. C., Balraju Vattikulla & S. Aravind "Total Digital Literacy Initiatives in Kerala: A Study of the Educational Digital Awareness Mission" 11 *Int'l J. Innovative Res.Tech.* 1518 (2024)

'middlemen' puts a person at risk, as they might transmit harmful cyber practices on the internet.[20]

VIII. Role Of Stakeholders In Cybersecurity Education– Government, Academia, Corporate, And Civil Society Collaborations

It will require the concerted efforts of multiple groups to ensure that cybersecurity education is promoted in India, with complementary contributions from each in the areas of infrastructure, awareness, and training. It is primarily the duty of the government, through the establishment of entities such as CERT-In and NCIIPC, to track cybersecurity within the country and to devise schemes and structures to monitor it. Projects such as PMGDISHA, Digital India, and the 2013 National Cyber Security Policy aim to develop sound cybersecurity practices and basic technological literacy among the general public. Alongside devising schemes, the government ought to undertake training sessions, awareness campaigns, as well as workshops, especially in rural and semi-urban regions with lower cyber awareness.[21] These initiatives are further reinforced through partnerships with private entities that provide support in terms of resources, expertise, and outreach.

Educational institutions have a very important role in developing skills and spreading knowledge. Educational institutions help in developing courses, projects, and community engagement activities on issues of cybersecurity. Collaboration between educational and business segments help in developing training modules and course curricula in line with industry requirements. The private sector, including technology and bank sector firms and other tech startups, helps out in developing training modules and developing tools necessary for users to apply good cybersecurity measures. At grassroots level, organizations from non-government agencies help out in developing knowledge of cybersecurity into easy-to-understand courses, like cybersecurity courses for women and other community groups. Cybersecurity knowledge could reach out to a larger mass of people in collaboration between the government, educational institutions, industry bodies, and civil society groups. It would help develop India into a digitally safe nation.[22]

IX. Developing A Community-Based Cybersecurity Framework For India – Recommendations And Implementation Roadmap

An integrated approach will be essential in formulating an extensive community-based cybersecurity plan in India. First of all, panchayats, schools, and self-help

[20] Kerala IT Mission, Digital Literacy Mission Annual Review, 2022.

[21] Rishesh Kumar Gupta & Abhishek Dewangan "Cyber Security Awareness Campaign Lacking in Rural and Urban Area of India: A Review" 8 International *Journal of Innovative Science, Engineering and Technology* 443 (2021).

[22] PwC India, Cybersecurity Governance and Stakeholder Collaboration, PricewaterhouseCoopers Report, 2023.

groups need to be employed in order to reach the rural and semi-urban segments of the country with local awareness campaigns that are multilingual and culture-specific. Capacity-building efforts need to focus on training not only in the basics of digital literacy but also in secure password use, phishing awareness, use of online funds transfer systems, and data protection methods. There needs to be a collective effort on the part of the government, the academe, the corporate sector, and the social sector entities in order to provide the necessary technical know-how and financial investment for cybersecurity purposes.[23] These can be made more engaging and accessible by technological interventions such as mobile-based micro learning modules, interactive apps, and easy-to-use reporting tools for cyber incidents. Other recommendations include integrating cybersecurity education in school curricula from an early age, regular readiness drills and simulations at the community level, and incentivizing participation through digital badges or recognition programs.[24] The establishment of regional cyber awareness and support centers can be focal points for education, research, and rapid response to regional concerns. Policy measures should encourage public-private partnerships for sharing resources, standardized reporting processes, and regular assessments of the effectiveness of programs. Finally, mechanisms for monitoring and evaluation must be a regular part of capturing the rates of adoption, measuring the outcomes of programs, and adjusting the initiatives for the constantly changing cyber-risks. This will allow India to develop a digitally aware, resilient, and proactive citizenry as a strong grassroots foundation of national cybersecurity and reduce the vulnerability of its growing digital ecosystem.

X. Conclusion And Policy Recommendations: Future Strategies For Sustainable Cybersecurity Capacity Building

A secure digital future for India requires a very carefully thought-out strategy that does not remain limited within the parameters of risk management. Cybersecurity in itself cannot be very effectively addressed by focusing only on technical solutions, but should be addressed by adopting a multi-dimensional approach that ensures the involvement of the public, learning, resilience, and dynamic legal systems.[25] With an added focus in the coming years, the need will be to shift more towards a preventive approach in cyber governance as opposed to focusing only on post-exposure solutions when faced with cyber events. Basic cyber awareness training within the curriculum of educational structures, professional training, and

[23] Tripathi, A. "Community-Based Cybersecurity Strategies in India: Bridging Awareness and Capacity Gaps" 19 *Journal of Indian Law & Technology* 6 (2022).
[24] Satya Narayan Mishra & Sanjaya Choudhary "Effectiveness of Cybersecurity Awareness Programs in Urban India: A Study in Cuttack" 5 *Int'l J. Advanced Res. Sci.,Comm. & Tech.* 182 (2025)
[25] Shriram D. Raut, Ashok R. Shinde & M. K. Patil "Cyber Security Awareness: A Movement of Digital Literacy Towards Making of Digital India" 11 *Ibmrd's J. Mgmt. & Res*. 174 (2022)

community-based training activities should become the focus for all future strategy plans for ensuring cybersecurity in the future.

Lastly, the deeper coordination among the central and state authorities with educational institutions, industry stakeholders, and civil society organizations is of prime importance in establishing a comprehensive, cohesive, and scalable cybersecurity framework.[26] Such coordination can avoid fragmentation, promote knowledge sharing, and assure long-term sustainability of initiatives.[27] Thus, India can build a digitally aware and resilient citizenry capable of protecting personal, institutional, and national digital assets by fitting education, technology, and participatory governance into a single vision. This approach becomes very realistic for developing a robust cybersecurity ecosystem that will meet future challenges with support for inclusive digital growth.

[26] C. Amal Chandra "Strengthening India's Cybersecurity and Data Privacy Regime" 3 *Indian J. Pub. Admin 3* (2024).

[27] Richa Sharma et al. "Digital Empowerment and Cybersecurity: Understanding Public Awareness of Digital India Initiatives" 102 J. *Theoretical & Applied Info. Tech.* 7763 (2024)

UTILIZING BLOCKCHAIN TECHNOLOGY TO STRENGTHEN INTELLECTUAL PROPERTY OWNERSHIP IN INDIA

Abhijay Singh[*]

ABSTRACT

Blockchain technology, considered revolutionary by some, has gained momentum over the past decade. Jargons such as Cryptocurrency, Bitcoin, NFTs, and many more have started to gain popularity amongst the public. People have become willing to adopt these new technological ideas into their fields. While some countries have integrated fintech fully into their legal system, others, like India, have been reluctant to put out defined regulations, and with good reasons. Yet the scope of blockchain technology remains vast. This article aims to analyse a lesser-researched topic. Many intellectual property owners in India face a large variety of issues regarding their ownership of the property. Administrative bottlenecks such as the lengthy duration of patent filing, copyright registration, etc., the extreme prevalence of digital piracy of intellectual property, and inadequate enforcement mechanisms of the central government and related bodies in enforcing their protection are only some to state. This article aims to recognise these ownership issues in India and how blockchain technology can quell many such issues prevalent within the country by integrating its features into the system. It will dissect how the various characteristics of blockchain technology, such as its decentralised nature and immutability, smart contracts, and privatised registries, will benefit Intellectual Property owners. It also observes existing issues with blockchain technology as a mode of intellectual property protection and explains the government's reluctance to legally recognise it, while also offering suggestions to counter these issues in order to successfully navigate the potential of this upcoming technology and deliver enhanced rights to the people.

I. INTRODUCTION

The law must adapt with the onset of modern technologies in order to ensure greater efficacy and leave no strings untied to ensure minimum exploitation of the people and thus, successfully serve its purpose. Blockchain technology, which gained popularity with the rise of cryptocurrency in 2009, has revolutionised many fields relating to technology. Its decentralised nature and distributed ledger technology, along with a plethora of other features, have made it versatile for implementation in several ways. The article highlights and analyses the ways in which blockchain technology can be used in order to strengthen the ownership of

[*] The author is a student at National Law University, Shimla, Himachal Pradesh, and may be reached at abhijaysingh05@gmail.com

intellectual property in India. India has multiple codes and statutes that govern intellectual property, but is also a member state of many international intellectual property protection agreements, such as TRIPS or the Paris Convention, to name a few. However, few of these agreements are fully followed through in the country, leading to some haphazard implementation leading to administrative and legislative dilemmas when it comes to the security of ownership of intellectual property. Patent filing, for example, may take up to 1 to 1.5 years to be completed fully after the new amendment rules. The problems do not stop there. There is a large influx of digital piracy in India, with it ranking as the third highest in the number of visits to illegal streaming sites in 2021.[1] This is detrimental to the enforcement of intellectual property rights in India and puts a halt to creativity amongst the populace. Many such persistent issues can be circumvented with the use of blockchain technology. However, the government is hesitant to enforce this mechanism with legal recognition.

II. CONCEPT OF BLOCKCHAIN TECHNOLOGY

The concept of Blockchain technology is far too vast to explore completely; thus, only the relevant details will be taken into consideration. First, we must understand how it works. A blockchain, as its name implies, is a chain of blocks. Each block has three main components. The first is data, which is often a record of transactions, but can vary from service to service. Next is the hash, which is a unique identification number of the recorded data. If the data on the block is altered, then the hash will also change, making it easier to track changes. The third component is the hash of the previous block. The last component enables tightened security of each block and serves as the connecting piece to the next block. If data is maliciously altered in one block, leading to a change in the hash, the hash of the previous block is always recorded on the next block, making it difficult to alter the data.[2] Lastly, the most well-known feature of the blockchain is its decentralized nature. The blockchain is not owned by a single entity, rather distributed over multiple nodes or systems. Each system has a participant whose job is to verify and update the ledgers.[3] This makes it so that if a person intends to alter data in a block, they will have to take control of the various nodes verifying it, making it exceptionally difficult to access data. In addition to this, blockchain makes use of a convenient but revolutionary feature: Smart Contracts. These are contracts that activate on certain conditions being fulfilled on the

[1] Patrick Kilbride, "Digital piracy jeopardises India's flourishing creative economy" *Times of India*, Nov. 6, 2022, *available at* <https://timesofindia.indiatimes.com/blogs/voices/digital-piracy-jeopardises-indias-flourishing-creative-economy/> (last visited on July 27, 2024).

[2] Justinia Taghreed, "Blockchain Technologies: Opportunities for Solving Real-World Problems in Healthcare and Biomedical Sciences" 27 *Acta Informatica Medica* 285 (2019).

[3] Christian Catalani and Joshua S. Gans, "Some Simple Economics of the Blockchain" 22952 *National Bureau of Economic Research* 14 (2016).

blockchain.[4] We will see how it can be applicable in the future sections. This technology has gained prominence in the field of data privacy and protection and can therefore be similarly used for intellectual property ownership, thereby strengthening intellectual property rights.

A variety of statutes govern intellectual property rights in India. They can be accessed either digitally, as in the case of copyrighted music, or physically, as in the case of a patented invention. The usage of blockchain need not be limited to the digital space. While its characteristics are best suited to tackle ownership issues of IP protection on the internet, it can be used to securely create and establish an IP right by digitalising much of the process and, in turn, streamlining it.

III. PATENT FILING AND OWNERSHIP

Let us take up the patent filing process covered in 'The Patents Act, 1970' and 'The Patent Rules, 2003'. Once a person has lawfully filed a patent, it can only be published after 18 months, unless a request is permitted under rules 24 and 24A, respectively. Further, under Rule 24B, a request for examination must be made within 48 months from the filing of the patent.[5] Even after this, a patent usually takes 2-3 years to be granted. Before its grant, anyone can create the very invention that the patent applicant. The process has too many hurdles to cross and unnecessary procedural delays. Using blockchain technology can significantly streamline the entire process.

A blockchain has the capacity to become a registry. The European Union themselves have created an IP Register based on blockchain, still in its nascent stage.[6] This is done by integrating the 'TMview' and 'DesignView,' which are flagship services of EUIPO for prior arts search to the blockchain and simultaneously updating it in real-time. The Indian equivalent of these services is 'InPass', which currently has no support for blockchain. If, like TMview and DesignView, InPass is also accommodated into the blockchain, then there could be a more secure and streamlined process of patent ownership.

The process would require using blockchain as a notary and the usage of smart contracts to record permanently in a register the proof of ownership. Firstly, an application must be filed with the necessary documents. Subsequently, the

[4] Alexander Savelyev, "Contract Law 2.0 'Smart' Contracts as The Beginning of The End of Classic Contract Law" 26(2) *Information & Communications Technology Law* 121 (2016).

[5] The Patent Rules 2003, r.24, r.24A, r.24B

[6] Tim Lince, "Innovation at the EUIPO: spotlight on digital tools and services" *World Trademark Review,* July 20, 2023, *available at* <https://www.worldtrademarkreview.com/data/ip-office-tools-and-services/ip-office-tools-and-services/article/innovation-the-euipo-spotlight-digital-tools-and-services> (last visited on July 27, 2024).

application would be encrypted onto the dedicated blockchain with certain keys and conditions. A notary in a blockchain serves as a legal checkpoint of sorts. When a patent gets stamped in the blockchain, it is notarized, meaning it has cryptographic proof of its existence.[7] This notarized application would then be submitted to the patent office for examination. After going through pre-grant opposition, if any, it would be recorded on the blockchain with approval of the patent. This adds transparency and an additional layer of verification, thereby strengthening the ownership of the patent.

So, what benefits do we get from encrypting a patent on the blockchain? This all seems like it can be done by the normal frameworks in place, so why go through the hassle of using blockchain and risking the impact of a decentralized filing system?

Under the normal patent filing process, one can write "Patent Pending" or "Patent Applied" under their invention; however, it is only to provide notice to the general public and cannot prevent them from replicating your invention as per Section 120 of The Patents Act.[8] On encrypting data using a smart contract, the information remains confidential in the initial stages. Granted, during the examination process, a patent is open to opposition; thus, it will reveal the nature of the invention. Still, an added layer of confidentiality can help protect a patent applicant's interests. Another point to be noted is that information gets timestamped on the blockchain. This prevents any administrative and human errors that can occur in the patent filing process, such as that which happened in Indian Patent No. 202639. In this case, the patent attorney failed to get an adequate payment done within the given timeline as per the patent rules.[9] Smart contracts also have the ability to notify alerts using different platforms, such as Tenderly.[10] Similarly, any issue regarding the delay of notification due to human mistakes can be easily overcome by providing timely notifications, which can be done through setting up keys on the smart contract as discussed.

IV. COPYRIGHT FILING PROCESS

The patent filing system, as per the research, is still done mostly offline, with records being kept in the blockchain for an added layer of ownership of one's

[7] Lulian, "Blockchain Based Notary Proof of Concept" *European Commission,* June 26, 2023, *available at* <https://joinup.ec.europa.eu/collection/blockchain-egov-services/solution/blockchain-based-notary-proof-concept> (last visited on July 28, 2024).
[8] The Patents Act, 1970, s.120
[9] Aparajita Lath, *"Professional Negligence and Attorney Liability?" Spicy IP*, Jan 23, 2014, *available at* <https://spicyip.com/2014/01/professional-negligence-and-attorney-liability.html> (last visited on July 28, 2024)
[10] Bogdan Habic, *"How to Set Up Real-Time Smart Contract Alerts with Tenderly," Tenderly*, May 18, 2023, *available at* <https://blog.tenderly.co/how-to-set-up-real-time-alerting-for-smart-contracts-with-tenderly/> (last visited on July 29, 2024*)*

invention. The Copyright ownership process finds itself to be more elaborate. There are a handful of things to consider, such as creating tokens, enacting smart contracts for royalties, and ultimately giving more control to the copyright owner, which has been touched upon by many researchers. This can be in part attributed to the fact that most copyrighted works are digital.

Non-Fungible Tokens play a key role in the process. NFTs, short for Non-Fungible Tokens, are digital assets that can be art, music, photos, or collectibles.[11] They gain credibility because they each contain a unique identity, much like a copyright.

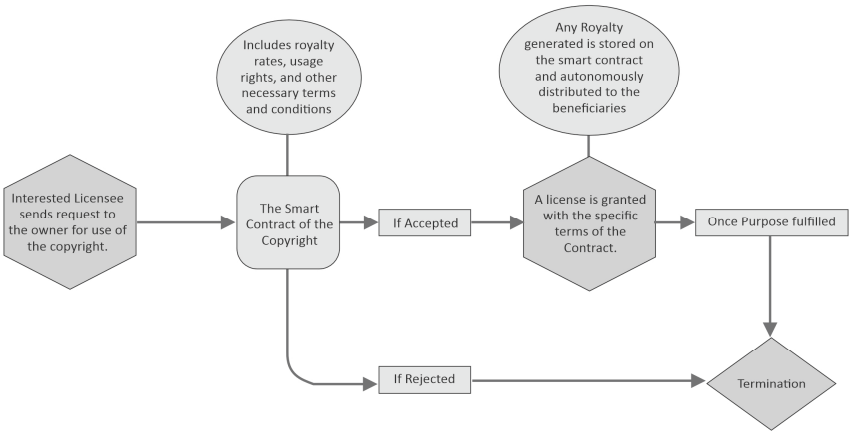
To initiate the process, one would have to create a digital token containing information about the person's work. For example, if an artist decides to publish a music track, they'd account for the data of the music, when it was created, and other integral information, whilst generating their token. Now this token will have to be recorded onto a blockchain with a specific use for copyright registration. This would need to be incorporated and updated via government notification under Section 44 and Section 45 of the Copyright Act, which pertain to the creation and maintenance of a register.[12] These sections don't specify the medium of the registry; thus, it can be updated to use blockchain with a government notice. In Kazakhstan, a similar initiative has been taken to protect copyright via the CARRIP platform. The system autonomously determines the price, and users receive a certificate, complete with data and a time-stamp based on the file's size.[13] Just as discussed in the patenting process, the Copyright claim will get timestamped, providing an extra layer of security and verification. Due to the decentralized nature of blockchain, the copyright claim, once approved and verified by the Copyright Office, can be seen by any person upon accessing the blockchain, thereby adhering to Section 47 of the Copyright Act of 1957.

The process also requires using smart contracts to license the copyrights. Smart contracts were considered revolutionary because they eliminated the need for a 3rd party to the contract, which would handle the licensing. Now the process if fully automated. This eases the issue of royalties and licensing. This can be explained in the following module:

[11] Alex Macura, *"NFTs & Copyright: What Do You Own?" Search Engine Journal,* May 19, 2023, *available at* <https://www.searchenginejournal.com/nft-copyright/481280/> (last visited on July 27, 2024)

[12] The Copyright Act, 1957 (14 of 1957), s.44, s.45, s.47

[13] Kelly Cromley*, "Future NFT Technology Introduced CARRIP: A Blockchain-Powered Intellectual Property Registry," Cointrust*, Feb 6, 2024, *available at* <https://www.cointrust.com/market-news/future-nft-technology-introduces-carrip-a-blockchain-powered-intellectual-property-registry> (last visited on July 27, 2024)



First, an interested licensee would request usage of the copyright from the owner. If it's accepted, then the licensee will have to fulfill the terms of the contract. This could include the payment needed to be made to the owner, or the specifications of usage. This makes possible numerous benefits, including greater transparency, elimination of a 3rd party, and prevention of any commission of error by humans in the collection, calculation, or distribution of royalties.[14] Other issues are tackled with the usage of smart contracts. Due to cross-border complexities, various authors would belong to different jurisdictions, and there can be issues with various copyright claims or licensing.[15] Such issues are resolved with a standardized copyright licensing process. This protects the owner's guarantee of their royalties and ownership over the copyright, ultimately strengthening their intellectual property rights.

V. DIGITAL PIRACY

Powering the copyrighting process via the blockchain also has benefits against digital piracy. Most intellectual property, like music, arts, or video games, find themselves on the digital medium. Subsequently, it becomes easier to pirate this intellectual property due to the various loopholes present in the digital medium, be it through hacking, torrenting, deep-web browsing, etc. Through the above-mentioned procedures, it is possible to effectively combat digital piracy.

- **Immutability -** The data is timestamped onto the blockchain. A hash is subsequently generated. On the next block, the previous hash is also

[14] S.F. Womba, M.M. Queiroz, *et. al*, "Dynamics between blockchain adoption determinants and supply chain performance: An empirical investigation" 229 International Journal of Production Economics (2020).
[15] Liu Y, Zhang J, et. al "Research on Digital Copyright Protection Based Hyperledger Fabric Blockchain Network Technology*" 7 PeerJ Computer Science (2021).*

recorded. Thus, if a malicious party does generate the correct hash, the hash on the next block will be altered. Thus, to completely mine a block, they'll have to guess the new hash on the next block as well. This can lead to insecure data, wherein the miners can form unions with stronger computational powers.[16] Thus, this study relies on a proof-of-stake system where validation is done by participants who offer collateral, or hold stake, and are constantly verifying the information of the block. The hash generation of the proof-of-stake method leads to an immutable nature, thus preventing copyright infringement.

- **No Single Point of Failure -** Due to the blockchain's decentralized nature, there is no single point of failure. For example, in a cloud system, failure of the cloud will lead to a collapse of the mechanism.[17] This becomes less probable in a decentralized environment where the data is constantly monitored across numerous devices and numerous validators.
- **Accessibility -** The blockchain enables users to manage authorized access to their data, as has been researched.[18] This provides an additional layer of security, combating access by digital pirates and also protecting important data.

To illustrate with an example, the movie 'Udta Punjab' was leaked completely before it was officially released. This was a tragic case of intellectual property infringement and was preceded by many others before it. There is no legal recourse to such cases, and it requires a John Doe order.[19] Similarly, when Balaji Motion Pictures Ltd. filed a suit against the various hosts of the streaming link for the movie, the High Court could at most give an order to terminate the links.[20] Even after this, streaming links were not completely taken down, directly disobeying the High Court's orders. Usage of a blockchain register for copyright would have easily prevented this. Piracy occurs when using a peer-to-peer file-sharing network. Any unauthorized movement of the copyright would immediately be flagged by the blockchain, and authorities could take preventive action. It would also become hard for insiders in the production to leak copies of the copyright if the smart contract has strict terms against its unauthorized sharing and distribution. Lastly, due to its digital watermarking, it can always record the

[16] Scott Nevil, *"What is Proof of Work (POW) in Blockchain?"* Investopedia, May 27, 2023, *available at* <https://www.investopedia.com/terms/p/proof-work.asp> (last visited on July 27, 2024).
[17] P. Fraga-Lamas and T.M. Fernández-Caramés, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry" 7 *Institute of Electrical and Electronics Engineers* 17580 (2019).
[18] S.H. Hashemi, F. Faghri, *et. al*, "World of Empowered IoT Users" *IEEE* 13-24 (2016),
[19] Rounak Biswas, "Udta Punjab and Online Piracy of Bollywood Movies" *BananaIP*, June 18, 2016.
[20] *Balaji Motion Pictures Ltd. v. Bharat Sanchar Nigam Ltd and Ors.,* (2016) SCC OnLine Bom 16029.

persons responsible for sharing and distribution of the copyright, thus offering a legal recourse by holding those directly responsible as punishable rather than unsatisfactory John Doe orders.

V. ASSIMILATION WITH INDIAN LAWS

So far, we have observed implementing blockchain technology for the protection of patent filing records and the protection of copyright itself. We can see their integration in the following ways: The Copyright Act, 1957 [21]
Section 13 - Copyright works should subsist original, literary, dramatic, musical, artistic, cinematographic, and sound recording works. All of these works can be encrypted onto blockchain technology.

Section 45-47 - This includes the registration process, wherein a register is to be maintained, which can easily be amended to be blockchain-powered. Moreover, due to the transparency of blockchain, any person can inspect the copyright as per the provisions of Section 47.
Significant amendments would have to be made to The Copyright Rules, 2013[22]. Rules 70 to 75 would have to be completely overhauled. These rules deal with the registration process of a copyright. They would have to be replaced by the methods discussed in this research. An issue we come across is in Rule 71, which deals with the correction and rectification of entries in the register. The copyright registrar has the capacity to take suo motu action or on an application to rectify any error. This is easy to do with editable digital resources. The blockchain prides itself on immutability; thus, a different measure would have to be adopted. Additional data would need to be added to the block containing data of the intellectual property, as one cannot overwrite it. This serves to be effective as it would always keep a record of any addition to change to the block and can be easily tracked. All in all, the Copyright rules would have to be massively revamped or have to be replaced with new legislations. The same case can be made for the Patent Rules of 2003, especially Rule 6 dealing with forms and contents of a patent application, Rule 11 dealing with publication and examination of patents, and Rule 20 specifying the form and patent specifications.[23]

V. THE ISSUE OF JURISDICTION

Jurisdiction seems to be one of the major obstacles when it comes to IP protection powered by Blockchain. One can use blockchain technology as valid legal evidence in court because of the trustworthiness of its time-stamp. These are verifiable and auditable records. However, it is decentralised, and that goes against the principles of international laws. To integrate it into the Indian legal system, many amendments would have to be made to the law. Secondly, a semi-

[21] The Copyright Act, 1957 (Act 14 of 1957), s.13, s.45, s.46, s.47.
[22] The Copyright Rules, 2013, r.70, r.71, r.72, r.73, r.74, r.75.
[23] The Patent Rules, 2003, r.6, r.20.

centralised model would need to be followed. The law would have to mandate coordination between the nodes of the blockchain, the regulators of the blockchain, the IP agencies of the government, and other necessary parties. This can become a hectic process and has no real solution aside from a rigid mandate on cooperation. This does, however, lead to cross-border complexities that can be dealt with due to the vast nature of the blockchain, but aren't provided for in international agreements.

V. Conclusion

Blockchain technology finds itself to be quite versatile in its uses, especially when it comes to safeguarding intellectual property. Considering the modern day, where digital piracy rates are at an all-time high, and people find it difficult to register their intellectual property due to administrative delays, features like smart contracts, immutability, and decentralization give that extra layer of protection to the IP holders. Despite the theoretical advantages of blockchain-based solutions, however, it must be carefully integrated into the Indian legal system. Collaboration of stakeholders, jurisdictions, and regulatory issues that arise as an outcome of the decentralized nature of the technology will need to be considered and navigated with precision. Policy-makers should explore the practical application of the technology to enhance intellectual property protection and ownership.

DIGITAL DISSONANCE: HOW LATE ADOLESCENTS IN INDIA NAVIGATE FREE SPEECH AND BELONGINGNESS ON SOCIAL MEDIA

Vedika Khanna [*] ***and Dr. Ambika Dutta*** [**]

ABSTRACT

This article explores how late adolescents in India shape their identities through social media and examines the relationships among digital civic engagement, mental health, and self-expression. Adolescents often share their opinions, experiment with different aspects of themselves, and seek social validation on platforms such as Instagram and X. In addition to that, they are also exposed to negative content, comparison, and criticism on these platforms. Legal frameworks such as the Information Technology Act and the Supreme Court Decisions often influence the presence of adolescents on social media and their online expression.

Based on Erikson's psychosocial theory of identity v. role confusion, Bandura's social learning theory, and Goffman's dramaturgical perspective on self-presentation, social media has been conceptualised as a performative stage in this article where adolescents can be seen navigating their authenticity, peer relationships and boundaries. Using a qualitative design, semi-structured interviews were conducted with 25 university students (aged 18–21) from Delhi-NCR. These interviews were analysed using thematic analysis, which led to the identification of several themes in digital self-expression, social validation and civic engagement.

Several key themes emerged from the thematic analysis conducted. Participants could often be seen negotiating between their authentic selves and their online presentation. This was a reflection of both self-exploration and impression management. Self-worth is often shaped by social validation received in the form of likes, comments, and followers. On the other hand, comparison often contributes to self-doubt and anxiety. Another relevant theme of "performative responsibility" emerged, where participants were balancing their need for free expression with awareness of legal responsibilities in the digital world. Finally, social media could also be seen as a platform for civic engagement as adolescents voiced their opinions on relevant socio-cultural discourses, gender, and politics. This highlighted the connection between identity expression and emerging forms of digital citizenship.

[*] The author is a research scholar at the NorthCap University and may be reached at vedika25psd006@ncuindia.edu

[**] The Co-author is an Assistant Professor at the NorthCap University and may be reached at ambikadutta@ncuindia.edu

I. Introduction

Adolescents' usage of social media platforms has massively increased in the current digital age and time, which has led to it becoming a major part of shaping their identity. They tend to rely on social media to explore and experiment, which further leads to self-definition. Indian adolescents are growing up in a society that is rooted in tradition while also adapting to globalisation. Social media provides them with a space for self-expression and civic engagement. Adolescents use platforms such as Instagram, X (formerly Twitter), and YouTube to share their opinions, have an online presence, and interact with peers across socio-cultural contexts. At the same time, these digital platforms are also spaces of self-comparison, judgment, and exposure to potentially harmful content. This can impact and also shape the adolescents' self-perception as also mental health.

According to the American Psychological Association (APA), identity is often referred to as an individual's sense of self, which can be defined by a range of physical, psychological, and interpersonal characteristics that have not been shared by another individual, as well as one's affiliations with other social, ethnic, or national groups. Identity is made up of one's life experiences, interpersonal relationships, emotions, and values. During late adolescence, identities are particularly evolving, as individuals are negotiating their intrinsic and extrinsic expectations as they try to be independent as well as belong with those around them. With the advent of technology, especially social media, it has become a mediating factor in the development of late adolescents. The online presentation of adolescents is often shaped through the external validation they receive in the form of interactions, likes, comments, follows, and reshares on their posts, which indirectly influences how they think and feel about themselves.

For late adolescents in India, social media can be seen as a mirror where they can explore different parts of themselves, engage with different ideas and opinions, and experiment with who they desire to be. It can be used to express their opinions, showcase their talent, and engage with others similar to them to form communities and groups with shared interests or around common social causes that they wish to advocate for. For example, on Instagram stories, reels, X Threads, adolescents often share their creative interests, social and political opinions, and reflections and commentaries on their personal, social, and professional lives.

Social media helps individuals feel a sense of belonging with others online and also helps them feel empowered, which contributes to the socio-emotional development of these individuals. Social media also contributes to heightening one's insecurities, leading to comparison with others online, exposure to misinformation, and online bullying. It has also been observed that those users who seek validation in the form of likes, comments, and reshares often experience

poor mental health outcomes such as low mood, anxiety, mood swings, difficulty concentrating on tasks, high irritability, low self-esteem, and poor self-concept.

The use of digital platforms for social engagement has become increasingly popular among youth. Using hashtags, online protests, and virtual engagement, adolescents have started global movements. This form of activism is popularly referred to as "hashtag activism", which has made civic engagement more accessible for the youth and challenged traditional ideas that exist about activism. In India, adolescents have actively participated in a wide range of online campaigns to raise awareness around mental health, environmental justice, and gender equality. This has led to a new wave of digital activism, which has completely redefined how adolescents express themselves through social media. Several movements, such as # Blockout2024, #IndonesiaGelap, and #EcoWarriors, are popular ones. #Blockout2024 was related to the blocking of celebrities and influencers who remained silent on the Gaza conflict, which was a major humanitarian crisis. This reflects how adolescents are actively using these digital platforms responsibly to bring about collective change. The #IndonesiaGelap in 2025 reflected how adolescents participated in challenging budget cuts, state repression, and neglect of personal interests using X. The #EcoWarriors campaign was used to encourage adolescents to adopt sustainable practices, which reflected how social media helps adolescents not only shape their identity and experiment with self-presentation but also cultivate a sense of agency and civic responsibility.

While online digital engagement provides adolescents with a sense of purpose and a community, it often also exposes them to toxicity, misinformation and bullying. This highlights the cost of digital engagement, which is the pressure to participate, perform, and conform with others, which can often blur boundaries between authentic engagement and social conformity. Being exposed to distressing news, hate speech, and debates can take an emotional and psychological toll on users. Blurring of personal and political expression online, more so, can lead to public scrutiny or harassment, which can affect how they perceive their freedom of speech. As adolescents navigate some of these challenges, the Indian legal framework plays a major role in informing them about what is permissible and ethical on these platforms. Online Expression in India has been shaped by several Supreme Court Judgements and the Information Technology (IT) Act 2000. These acts and judgments have defined what is permissible and what is not, and this particular Act has raised concerns around freedom of speech and privacy for many. The 2015 landmark judgment, *Shreya Singhal v. Union of India,*[1] struck down Section 66A of the IT, which had been previously criticised for criminalising online speech that was "offensive" or "annoying", which was a very

[1] AIR 2015 SC 1523

vague description for criminalising. The right to free speech in digital speech was reinforced through this Act, and it also influenced how adolescents perceived their rights online, which allowed them to engage with social media with a renewed sense of relief and freedom. Thus, it can be seen that social media has a major influence on late adolescents in India. It not only influences them from a socio-cultural perspective but also from a psychological and legal perspective. Hence, social media not only is a space for self-exploration and creativity for adolescents, but it also expects users to be engaged in a digitally literate and morally responsible manner by posing questions around authenticity, privacy, and safety in a digital world.

II. Review Of Literature

Adolescence is a crucial period of psychological development. Individuals struggle with issues of identity and belongingness during this period. Understanding how adolescents build their identities is a major area of research in psychology, especially in today's digital world.

The psychosocial development theory of Erik Erikson provides a foundational framework for understanding how adolescents' identities get constructed. Adolescence is a crucial developmental period marked by the struggle between identity and role confusion, according to Erikson[2]. During this time, individuals experiment and explore themselves, which helps them build a cohesive sense of self. Once the struggle between building identity and feeling confused about their roles is resolved, they can build a secure sense of identity[3].

Erikson went on to highlight that identity development is a long-term process[4]. It involves two major elements: integration into a moral world and the ability to make interactions with one's environment. These two elements work well together since a person's social identity is influenced by their place and function within larger social networks in addition to their personal characteristics [5]. As a result, identity formation encompasses both social and personal aspects, where relational connectedness and a sense of belonging are essential.

Erikson's theory suggests that peer relationships are very important in how adolescents form their identities. Ragelienė says that adolescents form their identities by interacting with friends who have views that are similar to or

[2] Erik H. Erikson, *Identity: Youth and Crisis* (W. W. Norton & Co. 1968).
[3] K. Chen, K. Lay, Y. Wu & G. Yao "Adolescent Self-Identity and Mental Health: The Function of Identity Importance, Identity Firmness, and Identity Discrepancy" 49 *Chinese J. Psych.* 53 (2007)
[4] Erik H. Erikson, *Identity and the Life Cycle* (W. W. Norton & Co. 1994).
[5] H. Salima & H. Fayza, *The Impact of Using Social Media on the Psychological Identity of Secondary School Students*, in *Second Forum on Traditional Social Domains* 384 (Univ. of Ouargla, Alg., Nov. 26–27, 2014).

different from their own[6]. The time spent with other people helps adolescents explain their views on the world, accept healthy norms, and reject those that don't match how they see themselves. Peer communication helps adolescents in having a safe place to think about who they are and what they want, which helps them find themselves and fit in with their peers.[7]

Comparing yourself to other people is a big part of Erikson's identity versus role confusion stage. Cherry says that adolescents often compare themselves to their friends to feel better about how they look[8]. This helps adolescents to work through their problems that come up when they want to be themselves but also want to fit in. They learn what their limits are as independent people while also trying to fit in with their peers. These comparisons can help get to know oneself and grow as a person, but they can also be harmful if they clash with your own values and cause you to feel confused or unsafe.

Elsayed has suggested that developing an identity as an adolescent means constantly balancing the need for personal freedom with the need to join a group[9]. According to Elsayed[10]adolescents' sense of who they are is greatly affected by how they see their place in society, which is similar to Erikson's ideas. Today, especially with the help of social media, this relationship is getting more complicated as adolescents deal with different, and sometimes conflicting, versions of themselves in real and virtual worlds.

All these studies show that forming an identity as an adolescent is a complicated process that is affected by both internal psychological processes and relationships with other people. Erikson always said that identity is not a single achievement but a relational and ongoing developmental process.

Albert Bandura's Social Cognitive Theory, which was built on his earlier Social Learning Theory, gives us another way to look at how adolescents learn and repeat social behaviours[1112]. Many years ago, Bandura suggested that people don't just learn from direct experience, but also by watching, copying, and modelling the

[6] Toma Ragelienė "Links of Adolescents' Identity Development and Relationship with Peers: A Systematic Literature Review" 25 *J. Can. Acad. Child & Adolescent Psychiatry* 97 (2016).
[7] Id.
[8] Kendra Cherry, "Identity vs. Role Confusion: Psychosocial Stage 5—Understanding Erikson's Theory of Psychosocial Development", Verywell Mind (Aug. 8, 2019*), available at:* https://www.verywellmind.com/identity-versus-confusion-2795735 (last visited on June 4, 2026).
[9] Wael Elsayed, *The Negative Effects of Social Media on the Social Identity of Adolescents from the Perspective of Social Work*, 7 Heliyon e06327 (2021).
[10] Id.
[11] Albert Bandura, *Self-Efficacy: Toward a Unifying Theory of Behavioral Change*, 84 Psychol. Rev. 191 (1977).
[12] Albert Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory* (Prentice-Hall 1986).

actions of others. His theory, which he called "reciprocal determinism," focused on how personal factors, behaviour, and the surroundings all affect each other. When it comes to how adolescents see themselves in the digital age, Bandura's idea says that social media is like a huge observational field. Adolescents watch their friends, family, and public figures who live different lives, have different beliefs, and have different identities. Adolescents' self-image and goals are shaped by the models they see through processes of attention, retention, reproduction, and drive. Self-efficacy, a key part of Bandura's framework (1977), also affects how adolescents talk about themselves online and how they understand what other people say about them. Bandura's idea that what you observe influences behaviour is supported by the fact that adolescents observe others and modify their online behaviour to align with what others expect of them. This influences what they post, which in turn influences whether they seek approval or face rejection.

Erving Goffman's Dramaturgical Theory conceptualises social interaction as a form of performance. This further contributes to the above-mentioned perspective. Using play as an example, Goffman said individuals manage their identities through their actions both on stage and off stage. Preparation, honesty, and authenticity is present backstage. On the other hand, performance happens on the frontstage, where individuals engage with one another publicly and perform socially appropriate roles.[13]

With the rapid growth of social media, these boundaries have become increasingly ambiguous. Researchers assert that online platforms have integrated the frontstage and backstage, compelling individuals to continuously manage their impressions by presenting perfected versions of themselves to diverse overlapping audiences[14]. For example, close friends and private messages serve as backstage spaces where individuals can communicate about themselves more confidentially. Conversely, Instagram posts and public accounts serve as a frontstage for public platforms that showcase an idealised self-presentation.[15]

Gilmore refers to this period, during which mental and physical barriers diminish, as a "hybrid social stage," characterised by the convergence of domestic and professional domains[16]. Adolescents are consistently conscious that they are

[13] Erving Goffman, *Daily Contact* (Xu Jiangmin et al. trans., Huaxia Publ'g House 1990).
[14] Shu Lv, *The New Development of Dramaturgical Theory in the New Media Environment: Taking WeChat Moments as an Example*, 10 Commc'n & Copyright 5 (2018); Hong Dai, *Self-Presentation in WeChat Moments: Real and One-Sided Role-Playing, Take 15 Young People as an Example*, 7 Southeast Transmission 69 (2017).
[15] Kevin Lewis, Jason Kaufman & Nicholas Christakis, *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. Computer-Mediated Commc'n 79 (2008); Zeynep Tufekci, *Grooming, Gossip, Facebook, and MySpace*, 11 Info., Commc'n & Soc'y 544 (2008).
[16] David M. Gilmore, *Goffman's Front Stage and Backstage Behaviors in Online Education*, 1 J. Learning Analytics 187 (2014).

under observation and evaluation as they navigate this environment. Bandura's observational mechanisms and Goffman's dramaturgical principles are evident in the way individuals present themselves on these platforms. Therefore, the digital self functions as a performance sustained through continuous comments, likes, and feedback from the public, all of which either reinforce or challenge the individual's constructed identity.

Together, these concepts provide a comprehensive framework for understanding how adolescents construct their identities in the digital age. Erikson's psychosocial perspective illustrates how the developmental tension between self-identity and role confusion is represented. Bandura's cognitive frameworks demonstrate how adolescents internalise observed behaviours and regulate their own expressions. Goffman's dramaturgical theory elucidates the manner in which identity is enacted within online contexts.

When adolescents use social media, it provides them with a place to learn from others, have conversations, and sometimes question who they are. This reflects how complicated identity development is for adolescents today. Self-formation is a continuous process affected by content online, socio-cultural expectations, and psychological needs

III. METHODOLOGY

3.1 Purpose

The current study is an examination of self-expression, belongingness, and perceptions of free speech on social media for late adolescents in India.

3.2 Research Objectives

1. To explore how social media influences identity formation among late adolescents in India.
2. To examine how adolescents navigate free speech and belongingness in a digital world
3. To understand the psychological and social consequences of a digital presence

3.3 Theoretical Perspective

The theoretical perspective of the current research is that of phenomenology, a philosophy that has been predominantly designed to explore and understand people's everyday lived experiences.[17] It involves the development of new meanings to inform, or re-orient, how we understand that experience.[18].

[17] G. Shosha "Employment of Colaizzi's Strategy in Descriptive Phenomenology: A Reflection of a Researcher" 13 *Eur. Sci. J. 1857* (2017).
[18] Sally Laverty "Hermeneutic Phenomenology and Phenomenology: A Comparison of Historical and Methodological Considerations" 2 *Int'l J. Qualitative Methods* 1 (2003).

Researchers who base their research on this approach are interested in comprehending the human experience, with a focus on elements of our existence that are important to us and make up our living environment.[19] By focusing on the participants' voices, the research aims to understand how adolescents experience and interpret their digital selves within a socio-cultural and legal framework. Erikson's theory looks at adolescence as a period of identity exploration, Bandura's theory looks at observational learning through models, and Goffman's dramaturgical theory looks at social interaction as a performance[20][21][22]. In all, these come together to form a strong foundation for this research. It helps explain the interplay between self-presentation, external validation and moral responsibility for an adolescent on social media.

3.4 Research Design

A qualitative research design has been used to explore adolescents lived experiences. Qualitative research is used for an in-depth analysis. Since this study is focused on meaning-making and identity processes, semi-structured interviews were chosen. This allows participants to openly share their experiences and talk more genuinely about their psychological needs and how they navigate their digital expression.

Quantitative measures could have been restrictive in nature. A qualitative approach helps explore how adolescents build and shape their identities.

IV. METHODOLOGY

4.1 Participants

The current study used purposive sampling. It included 25 university students aged 18–21 from the Delhi-NCRs region. Participants were representative of diverse academic backgrounds and social media usage patterns. The inclusion criteria were that they had been active users of at least two platforms (e.g., Instagram, X, Threads). This age group reflects late adolescence. This is usually a time period that is characterised by identity exploration and heightened digital engagement.

Sampling continued until data saturation was achieved. This helped ensure recurring patterns across narratives. Participants were recruited through university networks, peer referrals, and social media posts.

[19] Jonathan A. Smith & Michael Osborn, *Interpretative Phenomenological Analysis*, in *Qualitative Psychology: A Practical Guide to Research Methods* 53 (Jonathan A. Smith ed., Sage 2007).
[20] Erikson, *Identity*, supra note 1.
[21] Supra Note 11 at 86.
[22] Supra Note 13 at 87.

4.2 Procedure

Participants were contacted and provided an informed consent form. Individual semi-structured interviews were conducted online via Zoom. Interviews lasted 45–60 minutes each. They mainly focused on themes such as self-presentation, peer influence, online expression, and digital responsibility. Participants were informed about confidentiality, voluntary participation, and the right to withdraw at any point.

Interviews were recorded and further transcribed. Pseudonyms were assigned to the participants to protect their confidentiality.

4.3 Data Collection Tool

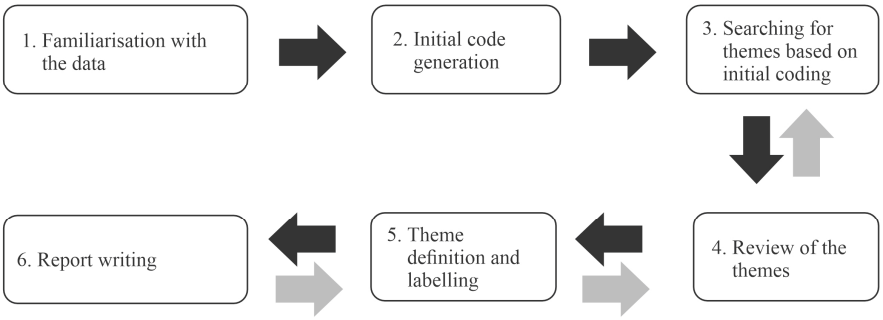
A semi-structured interview schedule containing open-ended, non-directive questions to encourage free narrative and detailed responses was used. The questions focused on the experience of participants describing their online self and authenticity, perceptions of freedom and boundaries in the digital world, role of social validation, experiences of comparison, judgment, and belongingness, and reflections on civic engagement. Responses were probed further for clarification. At the end of the interview, respondents were invited to add any additional comments to ensure their experience had been sufficiently covered. The interviews were audiotaped and transcribed verbatim. See Appendix for interview schedule.

4.4 Data Analysis

After transcription of the interviews, Thematic Analysis was employed to analyse and interpret the data. For this study, the inductive approach to thematic analysis was adopted, wherein the coding and development of themes were done from the data itself.

This approach to data analysis was used because it provides insights into the patterns of meanings across a given set of data, assisting in the discovery of shared meanings and commonalities in the participant experiences. The flexibility of thematic analysis was another reason for using it as a method of analysis, as it would allow the researcher to fulfil the exploratory goal of the study and ensure that the themes were data-driven and the interpretation of data is consistent with the participants' own accounts of their lived experiences.
The thematic analysis was conducted according to Braun and Clarke’s six-step approach:

Steps followed in thematic analysis:



Familiarisation with the data: This step involved reading and re-reading the transcripts to deeply familiarise oneself with the data. The researcher noted initial ideas in the margins of the transcript. Similarities with themes identified during the systematic literature review were also noted in the margins.

Initial code generation: A code is a label provided to the feature of data that is relevant to the research objectives. The unit of analysis was a 'sentence'. The 'sentences' varied in length, with some only being a few words long and others containing many words. At this stage, certain similarities were identified across the data set, and the first-level codes were extracted from the data. This stage ended with all the relevant data being coded and similar codes being identified across the transcripts.

Searching for themes based on initial coding: After the data were coded, the researcher moved to identifying potential themes. This was done by searching for common patterns among the codes and clubbing them into one theme, keeping the objectives of the research in mind. This was followed by the differentiation of sub-themes from main themes.

Review of themes: At this stage, the themes were reviewed by checking whether the data extracts (sentences made by the participants) fit well into them, which led to renaming and discarding of some themes.

Theme definition and labelling: Once the themes had been reviewed, renamed, and selected, each of them was defined in a sentence or two to state what was specific about them. Themes were analysed to produce the overall story of the data. Some points which were kept in mind while defining the themes were that each theme must have a singular focus, they must be related but not overlapping in nature and that they must address each of the research objectives. The names given to the themes must be crisp, clear and precise.

Report writing: This step involved the final analysis of the data and writing down the themes in the report. Vivid, compelling, supportive data extracts were selected, relating back to the research objectives and literature. It was ensured that the themes follow each other logically, such that they form a coherent, overall story of the data, in alignment with the research objectives.

Themes such as *curated authenticity*, *social validation and comparison*, *performative responsibility*, and *digital belonging* were derived as the themes from the process of thematic analysis.

4.5 Ethical Considerations

Participants were asked to participate voluntarily. Informed consent was taken, and confidentiality was maintained. Participants were given a brief about the study's purpose, assured that their responses would be used anonymously and informed that all the data collected would be stored securely. No monetary incentives were provided for the study. Participants were thanked for their contribution to understanding adolescent experiences in the digital era.

4.6 Reflexivity

The researcher maintained a reflexive journal throughout the study to make a note of any kind of biases and reflect on them. As a young adult navigating the digital world, the researcher's position facilitated rapport with participants. However, it was necessary to ensure that any assumptions or personal experiences did not clash with the process of interpreting participant responses. Thus, reflexivity ensured that interpretations of the study remained grounded in participants lived experiences.

V. Results And Data Analysis

This table represents the findings from semi-structured interviews that were conducted. These were conducted on 25 late adolescents (aged 18–21) from Delhi-NCR. The participants were made to reflect on their experiences on social media platforms like Instagram and X (formerly Twitter).

The interviews explored how participants experience their online and offline worlds, how online feedback and social comparison shape their sense of self, how they navigate freedom of expression, and how they belong and participate in a digital world. Erikson's theory of psychosocial development, Bandura's social learning theory, and Goffman's dramaturgical model of self-presentation were used to guide the analysis of their responses.

Four superordinate themes emerged from the data:

Major Themes	Subthemes	Key Interview Questions Linked
1. **Negotiating Authenticity and Performance**	- Self-exploration and emerging identity - Impression management and digital performance - Emotional fatigue	"How would you describe yourself on social media compared to offline?" "In what ways do you feel your online self reflects your true identity?" "Can you share an experience when posting made you feel you were exploring a new part of yourself?"
2. **Validation and Comparison as Emotional Economies**	- Social approval and recognition - Comparison and envy - Algorithmic awareness and performance pressure	"How do reactions from others such as likes, comments affect your sense of self?" "Can you describe a time when comparing yourself to someone online affected you?"
3. **Performative Responsibility and Digital Citizenship**	- Freedom of expression and self-censorship - Learning Responsible Expression - A Form of Digital Citizenship - Digital activism and moral agency	"How do you decide what opinions to share online?" "What does freedom of expression mean to you?" "Have you expressed your views on social or political issues online?"

4. Social Media as a Space of Belonging and Meaning-Making	- Finding emotional communities - Emotional burnout - Fragility of belonging	"Have you ever felt a sense of community through social media?" "How does that sense of belonging influence your participation?" "How has social media shaped your understanding of who you are?"

Theme 1: Negotiating Authenticity and Performance

Social media has been defined as a stage for experimenting with multiple selves by late adolescents. Adolescents can be seen balancing *authenticity* with *curation.* Based on Goffman's theory, adolescents have often viewed online interaction as a "front stage" wherein their performance is often managed on the basis of the social validation they receive from peers. The navigation between real and ideal selves can also be connected to Erikson's theory of identity formation.

1.1 Self-Exploration and Emerging Identity

Participants in the study described using social media as a canvas for exploration of different parts of themselves. They could also be seen looking at social media as a performative space to share and express their ideas, opinions, values, beliefs, and creative selves.

"In school, I was posting to fit in with other peers. Now my feed is more about who I want to be. I post my art as well as my opinions on important issues." (P-5)

"Every post is almost like an earlier version of me. Through my feed, one can make out who I'm becoming and have become over the years." (P-12)

These responses can be understood using Erikson's theory of identity formation. Late adolescents can be seen experimenting with different roles to establish a stable sense of identity.

1.2 Impression Management and Digital Performance

As a response to the question about online vs offline selves. Participants could be seen sharing their experience about how they often have to plan what becomes visible to others. This was consistent with Goffman's *front-stage behaviour*.

"Online I feel that I am more collected and put together. Offline I'm more raw, messy and unfiltered. Social media is like my editing, almost like my filtered version." (P-8)

"I would say my online presentation is not fake but I think it is definitely filtered somewhere. But I also like it that way because I get to choose. It allows me to decide which parts of me I want others to see. "(P-21)

These responses can be connected to *impression management*, as adolescents try to balance their authentic selves with the expectations of others around them.

1.3 Emotional Fatigue

To understand how this affects their offline selves, participants described experiencing emotional fatigue at times from the self-presentation and having to meet the expectations of others.

"There's so much pressure to be online, to catch up with the ever-changing trends, but even that feels performative now." (P-9)

"I sometimes take breaks from social media because it starts feeling like I am in the spotlight at all times and I have to keep selling myself to be liked by others." These responses can be connected with the idea of balancing both self-expression and self-curation. Adolescents are constantly pulled between authenticity and performance in the digital era.

Theme 2: Validation and Comparison as Emotional Economies

Likes, comments and shares all tend to influence how participants present themselves online. These feedback mechanisms also tend to have an influence on the self-esteem and motivation of an individual. This connects with Bandura's social learning theory of reinforcement and modelled behaviour. Many participants share their experiences of feeling an emotional high when they receive a positive comment or significant engagement, and a massive low when there are fewer likes or comments on their posts. Reduced engagement on content leads to feelings of inadequacy and self-comparison. Hence, external validation in the form of likes, comments, and reshares can be seen as emotional currency for participants, as it not only influences how they are feeling but also contributes to their engagement as well as self-concept.

2.1 Social Approval and Recognition

Participants could be seen associating likes and comments with emotional reassurance and social affirmation.

"When people engage with my content, it feels like I am being seen, noticed, valued, and appreciated." (P-17)

"Even though I say likes don't matter, but deep down somewhere I know that they do, it is like an online applause which feels special." (P-2)

These responses can be connected with Bandura's social learning theory, which talks about external feedback shaping internal motivation as well as perceived self-efficacy.

2.2 Comparison, Envy, and Emotional Regulation

When asked questions around comparison, participants shared both self-doubt and admiration for the work of others.

"It's honestly like a cycle, I sometimes get inspired by others. After some time, I start feeling less than them, which leads to feelings of inadequacy." (P-10) "Even though I know people post highlights and the best versions of themselves, sometimes I still do feel like I'm falling behind." (P-6)

These responses indicate how social media amplifies self-evaluation as adolescents engage in comparison with other people online.

2.3 Algorithmic Awareness and Performance Pressure

Participants also shared their experience of having to post in a very strategic manner to maintain their engagement online.

"If I don't post for a week, my reach drops. I have almost started thinking in algorithms. I don't care how I am feeling, sometimes I just post to maintain my reach and follower count." (P-11)

"I often post content that performs well irrespective of whether I connect with it or not. It is all about what works and what receives acknowledgement online. The pressure really gets to you at times, and you feel the urge to post content like others around you are posting to feel like a part of them and belong with the larger group. " (P-13)

These responses are a reflection of how the algorithm, as well as social media engagement, mediates identity formation of adolescence in the current digital times.

Theme 3: Performative Responsibility and Digital Citizenship

Participants could be seen relating to social media as both an empowering and a constraining space for self-expression. They shared that they experienced a sense of tension between free speech and what could be misinterpreted, censored, or receive backlash online. They also talked about an evolving sense of civic consciousness, which has been shaping their online presentation. This can be further connected to Bandura's theory as well as Goffman's performance management theory.

3.1 Freedom of Expression and Self-Censorship

Participants shared how they considered social media to be both liberating and constraining. Awareness of legal frameworks, social consequences, and peer engagement often tends to shape what they post and when they post it. Many participants also expressed how the freedom of expression feels controlled by both moral expectations from the social-cultural background they come from, as well as the legal boundaries defined by the Government. Participants seemed to have awareness of the Information Technology Act (2000) and recent Supreme Court judgments, which were also subconsciously influencing their social media engagement. They shared being more careful in sharing their political as well as social views ever since they became aware of several cases that caught attention.

"I do feel I can say what I wish to online, but only to a certain extent. After all the news that I have read about people getting into trouble for what they post and tweets that they make, I have started double-checking whatever I am posting and ensuring that my opinions do not hurt anybody in power. Even if I deeply believe in what I am writing, I am sometimes scared about it getting reported or being misunderstood by another person or community." (P-1)

"It's not even about mocking or troubling someone. I have seen people around me receive a lot of backlash for political opinions that they have shared. This has further made me cautious, and even though I express myself, I try to be as diplomatic as possible, as I do not want to get into any kind of argument or conflict with others." (P-19)

These responses indicate how individuals have become cautious in their engagement online, which is also an indication of civic reflexivity in digital behaviour.

3.2 Learning Responsible Expression - A Form of Digital Citizenship

Participants shared how they understood what not to post by observing other friends' posts getting reported, or celebrities or popular names in the online world facing public or legal backlash. This can be connected to Bandura's social learning theory, wherein individuals tend to learn by observing and modelling others' behaviour.

"When somebody in my circle gets called out for an insensitive post, it is almost like a lesson for everybody in our group. Sometimes I feel that we are learning more about digital responsibility and citizenship out of fear of what bad could happen to us rather than education. It almost seems necessary for schools to now include a part of this in the curriculum to avoid bullying and harassment online." (P-16)

"*Even though there is free speech and with the changes in the Information Technology Act, I still feel participation online comes with a sense of responsibility. I have become more aware of how my post can be interpreted by the public, which has made me either keep my opinions to myself or be politically correct whenever I engage." (P-10)*

It is clear from these responses that participants have learnt how to engage with social media in a responsible manner and that they tend to balance their authentic selves with the expectations of the norms and laws of society.

3.3 Digital Activism and Moral Agency

Many participants associated their social media usage with civic awareness and identity.

"Posting about gender issues always feels empowering. I feel deeply connected to the topic, and I feel like I am becoming a part of a larger movement that can lead to major change in society." (P-14)

"Social media was the place where I first learnt how to formulate my opinions and share them with others to receive their feedback. This process helps me become a part of larger movements and contribute to causes I feel deeply about." (P-4)

These responses reflect Bandura's concept of moral agency. Observation, reflection and participation become an integral part of civic identity development.

Theme 4: Social Media as a Space of Belonging and Meaning-Making

Social media provides individuals with a platform where they can connect with other individuals and form associations with those who have shared values, opinions, and interests, which has become very rare in the current offline space. However, this sense of belongingness is often fragile as it is influenced by emotional fatigue that comes with online engagement as well as the conditional nature of digital acceptance. Based on Erikson's theory, it can be noticed that late adolescents are able to resolve the conflict between belongingness versus isolation by connecting with others online.

4.1 Finding Emotional Communities

Participants were able to engage with communities and groups of people with common interests and shared struggles.

"I was able to find people whom I could relate to online. By following a conversation under an LGBTQIA+ post, I was able to connect with a group of queer folks, which made me find my people with whom I felt heard, seen and understood. I did not have to feel alone anymore; I finally had a place where I belonged." (P-15)

"Some of my online friends know me even more than my school friends. Even though I have never met them, I feel I can connect with them deeply." (P-25)

These responses are a demonstration of Goffman's theory, which talks about backstage behaviour, wherein participants can be seen disclosing parts of their authentic selves with complete honesty and freedom.

4.2 Emotional Burnout

Participants also share how they experience intense burnout after using social media for long hours continuously. Sometimes they scroll through really painful images or news with no felt experience of pain.

"I remember spending three hours continuously scrolling on Instagram when I was alone. To cope with the loneliness, I didn't even realise how fast the time passed. There were some really horrifying pictures on my feed, but I didn't feel anything. I was so numb to it all, I just felt like it helped escape the loneliness." (P-16)

"Despite feeling overwhelmed sometimes, I notice myself posting happy pictures to just maintain my feed. The contrast in the experience leads to further pain and tiredness." (P-20)

These responses connect with Erikson's theory, which talks about the conflict between identity versus role confusion as well as belongingness versus isolation.

4.3 Fragility of Online Belonging

Participants shared how online communities did provide them with a space for connection; however, they often felt quite conditional.

"Online friends are not permanent. One disagreement or drop in content leads to their disappearance." (P-22)

"Sometimes I feel that I only belong if I say something that is accepted by others. As soon as I say something unpopular, I am immediately blocked or bullied." (P-18)

These responses highlight the volatility of digital relationships. While it can be a place to find and build new connections, it can also be quite transient and risky.

VI. DISCUSSION

This study is an in-depth exploration of how late adolescents in India navigate their identity, sense of belongingness, and civic engagement on social media. The results from the study highlight the psychological and socio-cultural factors that influence adolescents' self-expression. These findings can be further explained by Erikson's Psychosocial theory, Bandura's social learning theory, and Goffman's dramaturgical model of self-presentation. The four major themes that came from the analysis of the participants' responses were Negotiating Authenticity and

Performance, Validation and Comparison as Emotional Economies, Performative Responsibility and Digital Citizenship, and social media as a Space of Belonging and Meaning-Making. This reflects that social media was both a source of empowerment and emotional vulnerability for the study participants.

Adolescents can be seen using social media platforms to explore different parts of themselves, experiment with their identities, and assert moral agency. While social media does provide adolescents with a space for self-exploration and self-definition, it also exposes them to pressures of performance, visibility, and conformity, which takes an emotional toll on them.

These findings can be further understood using existing literature. The literature demonstrates how identity formation among Indian adolescents is not merely an individual psychological process but is also shaped by social media engagement, peer influence, and evolving legal frameworks surrounding free speech.

6.1 Negotiating Authenticity and Performance

This theme was in alignment with Goffman's (1959) dramaturgical model. Adolescents could be seen viewing social media as a "stage" for managing and experimenting with multiple versions of themselves. They were not trying to deceive; instead, they were trying to curate authenticity in a manner that balances self-expression with societal expectations. As one of the participants in the study mentioned, *"*Every post is almost like an earlier version of me. Through my feed, one can make out who I'm becoming and have become over the years*." (P-12).* This idea of "becoming" aligns with what Erikson (1968) suggests in his theory. His view of adolescence is as a stage of identity exploration, where adolescents experiment and refine their emerging selves to become who they desire to be.

Participants described online experimentation as an empowering process, yet emotionally draining at times. For instance, *"*In school, I was posting to fit in with other peers. Now my feed is more about who I want to be. I lost my art as well as my opinions on important issues*." (P-5).* Participants also shared the pressure to constantly remain online to keep up with the ever-changing trends. They shared how they live in fear of missing a new trend in case they are inactive for a long period of time, which emotionally drains them. One of the participants stated, *"*There's so much pressure to be online, to catch up with the ever-changing trends, but even that feels performative now*." (P-9).*

Several participants also shared how they cope by self-regulation and taking regular breaks, even if it comes at the cost of missing out on some important trends or updates. One of the participants shared, *"*I sometimes take breaks from social media because it starts feeling like I am in the spotlight at all times and I have to keep selling myself to be liked by others*." (P-3).* These results indicate how Indian adolescents negotiate performance on social media and their authentic

selves. It also reflects how one's digital identity can often become a site of emotional labour, where one has to negotiate between online visibility and self-preservation.

6.2 Validation and Comparison as Emotional Economies

Social feedback mechanisms such as likes, shares, and comments take on the role of emotional currencies. These tend to shape how participants view their sense of self and contribute to their self-worth. Bandura's (1986) social learning theory can help explain how adolescents internalise external validation as reinforcement. One of the participants shared, *"*When people engage with my content, it feels like I am being seen, noticed, valued, and appreciated*." (P-17)*, while another participant admitted that, *"*Even though I say likes don't matter but deep down somewhere I know that they do, it is like an online applause which feels special*." (P-2).*

The same systems of validation can also become a major source of insecurity as well: *"*It's honestly like a cycle; I sometimes get inspired by others. After some time, I start feeling less than them, which leads to feelings of inadequacy*." (P-10).* This duality is reflective of the oscillation between feeling empowered and experiencing self-doubt, which gets intensified by the algorithm online. One of the adolescents in the study shared, *"*If I don't post for a week, my reach drops. I have almost started thinking in algorithms. I don't care how I am feeling, sometimes I just post to maintain my reach and follower count*." (P-11).*

In India, where being visible and desirable are integral parts of the culture to feel a sense of belonging, this kind of algorithmic shift affects an individual's self-concept and the development of identity.

6.3 Performative Responsibility and Digital Citizenship

Performative responsibility goes beyond personal self-expression into moral and civic realms. Participants talked about a new kind of digital moral agency, where one's freedom of speech is limited by the social rules, peer judgment, and the legal scenario. *"I do feel I can say what I wish to online, but only to a certain extent. After all the news that I have read about people getting into trouble for what they post and tweets that they make, I have started double-checking whatever I am posting and ensuring that my opinions do not hurt anybody in power. Even if I deeply believe in what I am writing, I am sometimes scared about it getting reported or being misunderstood by another person or community." (P-1).*

These results indicate how adolescents in the current age are aware of India's laws and the amendments made in them, like the Information Technology Act (2000) and the *Shreya Singhal v. Union of India* (2015) decision. Some of these have shaped how adolescents understand digital speech. One of the participants shared, *"It's not even about mocking or troubling someone. I have seen people around me*

receive a lot of backlash for political opinions that they have shared. This has further made me cautious, and even though I express myself, I try to be as diplomatic as possible, as I do not want to get into any kind of argument or conflict with others." (P-19). These experiences highlight how adolescents tend to be pulled between self-expression and surveillance. They often experience a tension between their personal beliefs and public accountability.

If we look at the results using Bandura's (2002) lens, these can be a reflection of vicarious moral learning, which means learning from watching others' actions and consequences. As one adolescent in the study shared, *"When somebody in my circle gets called out for an insensitive post, it is almost like a lesson for everybody in our group. Sometimes I feel that we are learning more about digital responsibility and citizenship out of fear of what bad could happen to us rather than education. It almost seems necessary for schools to now include a part of this in the curriculum to avoid bullying and harassment online." (P-16).* This indicates how adolescents observe others and internalise social norms. They have also highlighted the need to raise more awareness about safe usage of social media and the changes in the legal arena, so that they don't have to feel fearful. Instead, they can engage with content with full confidence and awareness.

Civic engagement can also be seen as an extension of identity exploration. Adolescents shared how empowering they find posting about social causes they connect to as it also makes them feel like they are taking responsibility at a young age to be a righteous, digital citizen: *"*Posting about gender issues always feels empowering. I feel deeply connected to the topic and I feel like I am becoming a part of a larger movement that can lead to major change in society*." (P-14).* Such responses indicate that social media helps adolescents not only express themselves but also feel connected to social issues and advocate for them in a responsible manner.

6.4 Social Media as a Space of Belonging and Meaning-Making

Finally, participants shared how they are able to connect with like-minded peers on social media, which makes them feel like they belong. Their identity is co-constructed with the meaning they make out of these interactions with the community and the belongingness they experience. One of the participants shared how, *"*I was able to find people whom I could relate to online. By following a conversation under an LGBTQIA+ post, I was able to connect with a group of queer folks, which made me find my people with whom I felt heard, seen, and understood. I did not have to feel alone anymore; I finally had a place where I belonged*." (P-15).* Adolescents often experience a sense of connection and feel safe in online spaces that are difficult to find offline.

While participants do experience connection and belongingness, it can sometimes feel quite fragile and conditional in nature. One of the participants shared how,

*"*Online friends are not permanent. One disagreement or drop in content leads to their disappearance.*" (P-22).* Another participant further echoed a similar sentiment, *"*Sometimes I feel that I only belong if I say something that is accepted by others. As soon as I say something unpopular, I am immediately blocked or bullied.*" (P-18).* Emotional overload also came up for a few participants: *"*I remember spending three hours continuously scrolling on Instagram when I was alone. To cope with the loneliness, I didn't even realise how fast the time passed. There were some really horrifying pictures on my feed, but I didn't feel anything. I was so numb to it all, I just felt like it helped escape the loneliness.*" (P-16).* These results indicate how digital engagement can make one feel connected and occupied at times, but at the same time also deplete one's energy and emotional resources. This can further lead to emotional fatigue and burnout.

Thus, even though social media promotes self-expression and connection, it can also lead to emotional exhaustion and burnout. Hence, adolescents must set boundaries, engage in selective withdrawal by muting content, unfollowing accounts, and curating content that aligns with one's authentic self as a means of self-preservation.

Across all four major themes, identity development can be seen as an ongoing psychological and socio-legal negotiation. Erikson's theory highlights the developmental need for identity formation and belongingness, which was evident through the findings of this study. In addition to that, Bandura's theory also depicted how observation and reinforcement can influence one's digital participation. Goffman's dramaturgical lens could be used to understand how authenticity is managed in a performative manner. Hence, social media becomes a play for adolescents to learn and grow and a stage for moral, civic, and emotional self-experimentation and self-construction.

In the current times, it has become quite necessary for one to be aware of the limits and freedom of what one can say online, which has added a unique socio-legal dimension to identity development in India. This is essential as adolescents are no longer passive recipients of what happens around the world but digital citizens who are not only actively participating in socio-political discourses but also contributing to bringing about relevant change.

VII. Conclusion

The current study was conducted to understand how late adolescents in India navigate identity, belongingness, and civic engagement with the use of social media. The study was aimed at understanding how adolescents balance authenticity and performance online, how social validation and comparison shape one's emotional experiences, how awareness of legal and moral responsibilities affects online behaviour, and how digital spaces facilitate a sense of

belongingness and meaning-making. Late adolescents aged 18-21 were interviewed, and thematic analysis was conducted to analyse their responses.

The four major themes that emerged from the study were Negotiating Authenticity and Performance, Validation and Comparison as Emotional Economies, Performative Responsibility and Digital Citizenship, and Social Media as a Space of Belonging and Meaning-Making. This was a reflection of the relationship that adolescents share with the digital world. Findings of the study suggest that adolescents view social media as both a site for self-expression and a space to self-experiment, where identity is constantly negotiated between one's authentic self and curated self. Validation and comparison often become emotional economies, and they tend to play a major role in shaping the self-esteem and self-worth of adolescents. Furthermore, awareness of socio-legal boundaries has further shaped how adolescents express their opinions and participate in civic and political discourse online. Social media is a space for adolescents to not only connect with others, form communities with those who are similar to each other, have shared interests, values, or advocate for a common social cause, which helps them feel a sense of belongingness. However, this belonging was often described as fragile and conditional in nature, which results in a tension between one's desire to connect and self-preservation, which can often lead to emotional fatigue and burnout.

In all, the study can be seen offering elaborate insights into the process of identity formation in late adolescents in India. It also highlights how this often gets influenced by psychological, social, technological, and legal factors. These findings have implications for mental health professionals, policymakers, and educators. It emphasised the rising need for digital literacy programs in schools, which include emotional regulation tools, civic and legal understanding of online expression, and how one can remain safe.

The current study also underscores the urgent need to transform adolescent digital engagement in India by strengthening legal literacy. While constitutional protections under Article 19(1)(a) guarantee freedom of speech and expression, the various restrictions under Article 19(2), along with statutory frameworks such as the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, also have a significant role to play in shaping the boundaries of online expression that is permissible. A critical gap seems to persist in adolescents' understanding of these legal provisions which can either lead to over-censorship as a result of fear of legal consequences or uninformed participation exposing them to liability. This makes institutionalising digital legal education within academic curriculum a necessity which would help young users with an improved understanding of their rights, duties, and liabilities in online as well as offline spaces. Furthermore, there is a significant need for policymakers to ensure that there is a balance in state

interests and individual freedom in the implementation of regulatory frameworks in a democratic society like India. Strengthening adolescents' legal awareness would assist in fostering more constitutionally informed digital citizens, where the exercise of free speech will be both responsible and protected by law.

Research in the future can further expand upon the results of the current study to understand how identity evolves in adulthood, how experiences differ between age groups, gender, cultural and socio-economic backgrounds. Additionally, it would be interesting to study the long-term effects of social media usage on an individual's self-concept and mental health.

ARTIFICIAL INTELLIGENCE REVOLUTIONISING JUSTICE: TACKLING INDIA'S JUDICIAL BACKLOG

***Yash Vats*[*] *and Kirti Rana*[**]**

ABSTRACT

India's judicial system faces a critical challenge: a growing backlog of cases that delays justice delivery. Traditional solutions like Alternative Dispute Resolution (ADR) have limited impact. This research explores the potential of Artificial Intelligence (AI) as a novel approach to address this crisis, specifically within the realm of judicial administration. The article acknowledges the inefficiency of the current system, highlighting the strain caused by judge shortages and a rising number of cases. This results in lengthy trials that erode public trust in the justice system. The urgency for creative solutions necessitates exploring AI, a technology that has transformed various industries. The article also delves into the international aspect of the same idea by closely observing the USA, UK, China, etc. AI's analytical capabilities can be harnessed for tasks like case management, document analysis, and evidence review, freeing judges for more complex legal matters. Predictive analytics can identify patterns in past cases to inform resource allocation and strategic decision-making. Additionally, AI can assist in risk assessment, potentially leading to more effective decisions. Data privacy is a paramount concern when employing the use of AI. The research emphasises the need for robust data security measures and adherence to legal frameworks to safeguard personal information collected during investigations and trials. Finally, the research underscores the crucial role of human oversight. AI should function as a tool to empower judges, not replace them. Legal judgments require human experience, empathy, and ethical considerations that AI cannot replicate. By acknowledging the challenges of data privacy, algorithmic bias, and the irreplaceable role of human judgment, the article advocates for a measured and responsible integration of AI. This synergy can create a pathway toward a legal framework that is more streamlined, enduring, and fair.

I. INTRODUCTION

The primary problem facing the Indian legal system at the moment is the enormous backlog of unresolved cases at all judicial levels, from Lower Courts to the Hon'ble Supreme Court of India. It has lately been stated that the judicial system would disintegrate and become nearly meaningless if early action is not taken. Even worse than that is the loss of public confidence in the legal system. Justice needs to be done quickly, as "Justice postponed is justice denied." Every year, millions of individuals fail to avoid or resolve the most serious concerns connected to justice.

[*] The author is an Advocate and may be reached at yashvats147@gmail.com.
[**] The Co-author is an Advocate and may be reached at kirtifrankrana@gmail.com

The institutional justice mechanisms do not adequately address their needs for justice. As to the results of HiiL's Justice Needs and Satisfaction Surveys (JNS), conducted across over 16 nations, an average of just 33% of individuals are able to address their legal difficulties completely. 11% can address justice concerns to some degree, whilst 31% still struggle with them. 22% are unable to solve the problem.[1] A typical conflict settlement process makes use of both official and informal dispute resolution techniques. According to statistics from JNS polls, around 80% of individuals use informal judicial channels to address their legal difficulties. These can be elders living in the neighbourhood, friends, relatives, neighbours, or religious leaders. It's still challenging to comprehend how formal and informal judicial institutions are related to one another. The dearth of information on the outcomes of informal judicial proceedings makes it difficult to evaluate their effectiveness. According to research by the Supreme Court of India titled "Subordinate Judiciary-Access to Justice 2016," capacity limitations are the main reason for the high level of pendency.[2] In outlining the causes, the report claims that one important factor is that the subordinate judiciary is now working with a scarcity of courtrooms and judicial officers since not all subordinate courts have benefited from modernisation and computerisation. The backlog of cases in lower courts has increased as a result. As a result, justice is served in an ineffective and delayed way that is detrimental to all societies.

The integration of artificial intelligence (AI) is causing a transformational wave in the legal environment of the twenty-first century.[3] With the ongoing progress of technology, India's legal system is about to undergo a major transformation. This article explores the many applications of artificial intelligence (AI) in the legal field, looking at both the advantages and disadvantages of this innovative integration. India is not an exception to the growing importance of the relationship between artificial intelligence (AI) and the legal system. The application of AI in the legal sector has the potential to completely transform the way justice is administered as the nation advances technologically, but it also presents some difficulties that must be carefully considered.[4]

II. AI Applications In The Legal System

Artificial intelligence (AI) isn't just about fancy robots. It's the concept of building computer systems that can tackle tasks typically needing human smarts. This

[1] J. A. Siani "Empowering Justice: Exploring the Applicability of AI in the Judicial System" *J. L. & Legal Rsch. Dev.*, 24–28 (2024)
[2] *Ibid*
[3] Aishwarya Sharma et al. "Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges, and Ethical Implications" *5 SDGs Rev. 1* (2025)
[4] P. Jain "Artificial Intelligence for Sustainable and Effective Justice Delivery in India" 11 *OIDA Int'l J. Sustainable Dev.* 63 (2018)

includes understanding spoken language, interpreting what we see, making decisions, and even translating languages. In simpler terms, AI is about giving machines the ability to think and act like humans, or at least mimic our "thinking" processes like learning and solving problems. Artificial intelligence has proven beneficial in almost every field, including but not limited to healthcare, education, marketing, and defence.[5] AI is helping with medical diagnoses, medication administration, pharmaceutical formulation, treatment planning, and health record management. The Legal System uses AI in various ways, including

i. Legal Research and Analysis: The ability to do legal research has been greatly improved by AI-powered technologies. With the use of machine learning algorithms, advocates may quickly and more thoroughly understand legal precedents, legislation, and case law by sorting through enormous datasets. This quickens the legal analysis process and empowers professionals to make wise choices.[6]
ii. Contract Review and Due Diligence: AI is being used extensively in India for procedures related to contract review and due diligence. AI systems can evaluate contracts, spot any issues, and guarantee compliance rapidly, saving legal practitioners time and money.
iii. Legal Process Automation: By automating repetitive legal duties, AI is simplifying the legal process. Artificial intelligence (AI) is used in legal process automation to manage repetitive and rule-based processes, including scheduling, case management, and document writing. This lessens the workload for legal practitioners and increases overall workflow efficiency while lowering the possibility of mistakes.
iv. E-Discovery and Data Management: AI is essential to e-discovery and data management in the era of digital information. Massive amounts of electronic data may be swiftly and precisely sorted through by AI algorithms to find pertinent facts for court proceedings. This guarantees that relevant material is delivered on time and speeds up the discovery process.[7]
v. Chatbots and Virtual Legal Assistants: AI-driven chatbots and virtual legal assistants are becoming quite common.[8] These tools help solicitors by answering common questions, giving clients legal knowledge, and giving advice on procedural issues. These AI apps increase accessibility and enhance customer interactions, but they do not replace human knowledge.

[5] B. Jaya Prakash & N. R. Putchala, *The Automation in the Indian Judiciary*, 2821 *AIP Conf. Proc.* (2023)
[6] M. R. Sharma, *Artificial Intelligence in the Indian Judiciary: Current Applications and Future Prospects*, 33 *J. Namibian Stud.: Hist. Pol. Culture* 3479 (2023).
[7] Shatakshi Dixit et al. "Incorporating Artificial Intelligence into India's Judicial and Law Enforcement Systems" 7 *Int'l J. Multidisciplinary Res.* (2025)
[8] Ibid

vi. Predictive Analytics: Using past case data, AI systems use predictive analytics to predict legal outcomes. Although this might help attorneys plan their cases, it also calls into question the fairness and interpretability of such algorithms, particularly given the varied legal environment in India.[9]

III. Modes Of Artificial Intelligence In The Judiciary

3.1 *AI Integration in the Indian Legal System*

The eCourts Mission Mode Project[10] is a pan-Indian endeavour aimed at modernising the judiciary through technology. " By providing courts with ICT and automating processes, the initiative seeks to increase judicial efficiency and increase transparency in the Indian legal system. The first phase of the project, which took place between 2011 and 2015, involved preparing some court buildings and judicial service centres so that the district courts could implement computerisation. Union Law Minister Kiren Rijiju acknowledged that Phase III of the project, which began in 2015, will require the adoption of novel, cutting-edge technology like artificial intelligence (AI) because Phase II is coming to an end.[11]

Significant progress has been achieved in recent years, despite the glacial speed at which AI technology has been integrated into the legal system compared to other nations like China and the USA. The Supreme Court's 2021 introduction of SUPACE (Supreme Court site for Assistance in Court Efficiency)[12]The first artificial intelligence (AI) site marked a key turning point. By combining judicial procedures that can be automated using artificial intelligence, this portal seeks to identify those that require automation and assist the court in decreasing pendency and increasing efficiency. Since 2021, the Indian Supreme Court has processed data and given judges access to it for decision-making through the use of an AI-controlled device. It refrains from participating in the decision-making process.[13]

SUVAS (Supreme Court Vidhik Anuvaad Software), a system that translates court papers from English into regional dialects and vice versa, is

[9] Ibid
[10] Ministry of Law & Justice, Government of India, *E-Courts Mission Mode Project* (Dec. 17, 2024)
[11] S. Narayanan, M. Agarwal & S. Bansal, *Artificial Intelligence Inroads into the Indian Judicial System*, in *Legal Analytics* 35 (Chapman & Hall/CRC 2022)
[12] P. Nagpal "Use of AI Tools like SUPACE in Indian Judiciary: Constitutional Safeguards for Due Process and Judicial Independence*" 14 Int'l J. Eng'g Dev. & Res. 98 (2026),*
[13] Supra 1

also used by the Supreme Court of India.[14] In the case of Jaswinder Singh v. State of Punjab[15], the Punjab & Haryana High Court refused a bail motion because the prosecution had demonstrated the petitioner's involvement in a brutal, fatal attack. The sitting court consulted ChatGPT for its views to obtain a more comprehensive perspective on whether bail should be granted when cruelty is involved.[16] It's important to note that the trial court will not examine these statements, and that the mention of ChatGPT does not imply that the case's merits are being discussed. The reference was merely intended to provide a more thorough understanding of bail.

In Christian Louboutin *SAS & Anr. v. M/s The Shoe Boutique – Shutiq,* the Delhi High Court held that, given current technological advancements, artificial intelligence ("AI") cannot replace human cognition in the adjudication process.[17] It was emphasised that judgements rendered by AI chatbots cannot serve as the basis for factual or legal arguments in court.[18]

There were some raised eyebrows when the Supreme Court used the term 'common-law marriage' from Wikipedia to define 'a relationship like marriage' under the Protection of Women from Domestic Violence Act, 2005. *D. Velusamy v. D. Patchaiammal*[19] was the said case where such expressions were used? Even the source of ChatGPT's bail jurisprudence in this specific case is unknown to us. Therefore, the P&H High Court's citation to ChatGPT jurisprudence was superfluous. Courts should refrain from taking any acts that might seriously jeopardise someone's life, liberty, or property because they have an honourable duty to administer justice.

3.2 *Predictive Analysis in the United States of America*

AI is making its way into courtrooms with tools designed to help judges make decisions. One example is COMPAS (Correctional Offender Management Profiling for Alternative Solutions), which analyses a defendant's background, including social and economic factors alongside criminal history, to predict the risk of them committing another crime in the future.[20] Similarly, the US

[14] Kaveri Aditya Deo, *Artificial Intelligence Lifting Burden of Justice Delivery System in India*, 3 *Advances in Consumer Research* 1538 (2026)
[15] CRM-M-22496-2022
[16] Supra 8
[17] Rahul Hemrajani, On Non-Conventional Marks and ChatGPT Evidence: A Case Comment *on Christian Louboutin SAS v. The Shoe Boutique (2023), 19 Indian J.L. & Tech. Art*. 5 (2023)
[18] 2023 DHCc 6090
[19] 2010 SCC 10 469
[20] Jennifer L. Skeem & Jennifer Eno Louden, *Assessment of Evidence on the Quality of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)* (Univ. of Cal., Irvine, Ctr. for Evidence-Based Corr., Report for the Cal. Dep't of Corr. & Rehab. Dec. 28, 2007)

Sentencing Commission uses AI to develop sentencing guidelines that aim for fair and consistent punishments.[21] The US court system uses chatbots to answer frequently requested questions from the public on schedules, court procedures, and other relevant subjects. This reduces the effort of court staff members and enhances information accessibility for all parties.[22]

3.*3 Smart Court in China*

In China, AI helps judges streamline their work by digging through past cases and legal references relevant to the case at hand. This assistance doesn't stop at research; the AI can even suggest appropriate penalties based on similar situations that set a legal precedent. This translates to faster and potentially more accurate rulings for all the stakeholders involved in the case. Chinese courts employ AI to research cases as well. The 'China Judgements Online' service, powered by artificial intelligence, makes it simple for judges to find relevant court documents.[23]

3.4 Digital Case System in the UK

The Digital Case System for the Crown Courts was introduced by the UK Ministry of Justice in 2020.[24] It offers digital evidence submission, virtual court participation, and real-time case updates to reduce the amount of paper used. Criminal law solicitors use the online portal by following guidelines issued by the Bar Council's Ethics Committee.[25]

3.5 *Colombia ChatGPT Judgment*

Justice Juan Manuel Padilla of the Colombian court recently issued a decision using the ChatGPT AI technology. He was handling an insurance claim for an autistic child. Justice Padilla asked the ChatGPT bot, "Is an autistic minor exonerated from paying fees for their therapies?" and the bot gave him a response he thought acceptable. Justice Padilla then incorporated the conversation in his verdict. Thus, in compliance with Colombian law, he decided that a child with autism was not obliged to pay for therapy. Furthermore, Judge

[21] A Case Study on COMPAS Recidivism Data, 11 *Int'l Rsch. J. Eng'g & Tech.* 726 (2024)
[22] Bhutoria, A. (2022). Personalized Education and Artificial Intelligence In the United States, China, And India: A Systematic Review Using a Human-in-the-Loop Model. *Computers And Education: Artificial Intelligence*, *3*, 100068.
[23] Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, And Regulation. *Ethics, Governance, And Policies in Artificial Intelligence*, 47-79.
[24] Bar Council Ethics Comm., *Use of the Crown Court Digital Case System* (Dec. 2021)
[25] Sivasankar, S. (2024). A Comparative Study on Artificial Intelligence and Courtroom Practices in India, UK, And USA. In *Demystifying the Dark Side of AI in Business* (Pp. 1-19). IGI Global.

Padilla stated that AI does not replace judges as sentient beings.[26]

IV. LEGISLATIVE FRAMEWORK AND ARTIFICIAL INTELLIGENCE

In India, there are currently no specific laws governing AI. The Ministry of Electronics and Information Technology (MEITY) is leading the charge on developing an AI policy framework. They've established committees and partnered with Niti Ayog to create a set of seven principles for responsible AI development, focusing on areas like fairness, transparency, and data privacy. This focus on privacy is crucial because the Indian legal system, through the Supreme Court and subordinate courts, prioritises upholding fundamental rights like privacy. Existing data protection measures reside within the Information Technology Act, 2000, but a new Act, the Digital Personal Data Protection Act 2023, which has been passed by MEITY, has been passed to further safeguard individual data collection by both private and public entities. Considering the pertinence of data in the present times, this Act is a step in the right direction.

V. CHALLENGES IN THE CONTEXT OF THE LEGAL SECTOR AND ITS RECOMMENDATIONS

i. Data Privacy and Confidentiality: To learn and anticipate, artificial intelligence (AI) systems often require vast volumes of data. Sensitive information, such as financial or personal data, may be included in this type of data. The need for this kind of data for AI algorithms to properly train might make it difficult for businesses to abide by data privacy regulations.[27]

ii. Artificial Intelligence Bias: During training, bias in AI systems may manifest itself in the system's output. AI outputs may merely reproduce past and contemporary societal injustices rooted in gender, caste, ethnicity, and ideology, leading to outcomes that are not really meritocratic.[28]

iii. Licensing Accountability: Unlike qualified attorneys, AI systems are exempt from professional norms of conduct and ethical standards as they do not need to get a licence to practise law. It is unclear who should be held accountable or liable if an AI system produces wrong or deceptive legal advice. Even if judges still have the last say in matters of decision-making, the use of AI in the legal system presents issues. Because of

[26] Purvish M. Parikh, Dinesh M. Shah & Kairav P. Parikh, *Judge Juan Manuel Padilla Garcia, ChatGPT, and a Controversial Medicolegal Milestone*, *Indian J. Med. Sci.* (2023)
[27] T. Solanki, *AI and Technology in the Indian Judiciary: A Step Toward Efficient Justice Delivery*, *J. LEGAL TECH. & POL'Y* (2026)
[28] Manvee. (2023). Predictive Justice with Artificial Intelligence: Enhancing Efficiency and Accuracy of the Judiciary. *Legal Spectrum J.*, *3*,1.

automated bias, it is not commonplace to grow unduly dependent on technology-based recommendations.[29]

A New York lawyer got in trouble for using an AI tool called ChatGPT for legal research in a lawsuit. They included citations for fake cases in a court brief, but opposing lawyers couldn't find them. The lawyer admitted they didn't check the citations themselves. The judge penalised the law firm $5,000 for this mistake. As a result, while employing generative AI for legal research, attorneys should exercise caution.[30]

iv. Other issues: Because AI can learn on its own, it doesn't need the help of programmers or coders to operate. However, this might result in disparities in technology and the economy that remain unclear as of now. These differences might lead to data exploitation and undermine the basis established by the Competition Act of 2000. Ascertaining the culpability for technical errors in the legal domain may be a challenge. People's freedom and quality of life will be greatly impacted by the repercussions of AI-based errors. Nonetheless, when employing AI in their job, legislators and corporate executives in the legal and other fields need to be proactive in establishing accountability and defining distinct power structures. It's essential to remember that artificial intelligence should support legal work, not replace it. While AI is capable of streamlining laborious and time- consuming processes, it is not capable of handling legal counsel, strategic decision-making, or sophisticated legal analysis.[31]

VI. CONCLUSION

An intriguing potential for efficiency and creativity is presented by the introduction of AI into India's judicial system. But it needs a well-rounded strategy that takes into account moral issues, protects data, and encourages technology usage in a responsible manner. To fully use artificial intelligence in the service of justice, politicians, engineers, and legal experts must work together as India navigates this rapidly developing frontier.[32] AI-related problems and challenges include ethical dilemmas, prejudice, discrimination, privacy infringement, and security concerns. To address safety concerns in AI development, a global group of experts from the World Ethical Data Foundation (WEDF), which includes members from tech giants like Google, Meta, and

[29] Awasthy, S., Babu, P., & Singh, S. (2022). Application Of Artificial Intelligence and Machine Learning In the Indian Legal System: Use Cases For Judiciary, Law Firms, And Lawyers. *Part 2 Indian J. Integrated Rsch. L.*, *2*, 1.
[30] Supra Note 31 at 113.
[31] Supra Note 3 at 107.
[32] K. Singh, *Artificial Intelligence and Cyber Security in the Judicial System*, *Nat'l J. Cyber L. & Sec.* (2026).

Samsung, proposed a voluntary framework. This framework consists of 84 key questions that developers should consider at the outset of any AI project.

But as AI is used more often, the need for specialised laws to control the technology, get rid of inherent or acquired bias, and deal with ethical concerns is growing. Policies, guidelines, and white papers have been developed by jurisdictions such as the UK, USA, and EU to eliminate algorithmic biases and assess algorithmic effects. The European Parliament has made amendments to the Artificial Intelligence Act, 2024. Except for law enforcement, the proposed amendment would prohibit the use of artificial intelligence (AI) in biometric surveillance. It would also allow generative AI systems, like ChatGPT, to divulge content created by AI only with court authority. Therefore, keeping in view the best practices of other countries, India must tackle the challenges associated with artificial intelligence. There is an urgent need for robust data security measures and adherence to legal frameworks to safeguard personal information collected during investigations and trials. While framing guidelines related to AI, it needs to be remembered that the crucial role of human oversight cannot be missed.

AI should function as a tool to empower judges, not replace them. Legal judgments require human experience, empathy, and ethical considerations that AI cannot replicate.[33] By acknowledging the challenges of data privacy, algorithmic bias, and the irreplaceable role of human judgment, the research advocates for a measured and responsible integration of AI. This integration has the potential to pave the way for a more efficient, sustainable, and just legal system.

[33] Artificial Intelligence in the Indian Judiciary: A Systematic Analysis of Potential Applications and Challenges in Addressing Case Backlogs, 1 *J. Trends & Challenges in Artificial Intelligence* (2024)

NCU LAW REVIEW

Vol. 8, Issue 1 (2026)

ISSN: 2581-7124

SUBMISSION OF RESEARCH PAPERS

REVIEW POLICY

NCU Law Review believes in the encouragement of critical analysis and the interdisciplinary study of law. Submissions that view the subject matter from a comparative perspective shall be preferred. Therefore, the scholastic quality of the manuscript shall be the primary criterion for publication. The same shall be judged by an anonymous peer review of the manuscript. However, the final discretion as to the acceptance of the manuscript rests with the Editorial Board.

PUBLICATION POLICY

NCU Law Review publishes original material. Therefore, manuscripts must neither be under consideration for publication in any other place at any time during the period of consideration by the Journal, nor previously published. The Law Review also has a strict policy on plagiarism. Plagiarism shall render the manuscript liable for rejection.

SUBMISSION OF CONTRIBUTIONS

Contributions for the Law Review are solicited under the following heads:

1. **ARTICLES:** An article is expected to include a comprehensive review of the existing law in a particular area of study, and is conservative in both choice and analysis of subject. The subject matter is expected to be dealt with in a detailed and thorough manner.

2. **ESSAYS:** Essays are usually more adventurous, challenging existing paradigms and innovatively addressing well-known problems. An essay doesn't need to be as comprehensive as an article, and it is strongly recommended that essays be considerably more concise, in terms of scope and conceptualization.

3. **CASE COMMENTS:** A study of any contemporary judicial pronouncement (Indian or foreign) must contain its analysis, the context in which the particular judgment has been delivered, its contribution to existing law, and must necessarily comment on the judicial process involved.

4. **LEGISLATIVE COMMENTS:** This entails a critical analysis of any existing Indian legislation or proposed bills, and their constitutional implications. The analysis is expected to be original and technical in nature.

Contributions should adhere to the following specifications:

1. **WORD LIMIT:** The word limit for articles and essays is between 7,000 to 8,000 words (inclusive of footnotes), while case/legislative comments must be confined to less than 3,000 words.

2. **CITATION FORMAT:** The citation format to be used is INDIAN LAW INSTITUTE. Speaking footnotes are generally discouraged.

3. **ABSTRACT:** Every submission must be accompanied by an abstract of not more than 200 words, which outlines the area of study and any important conclusions that may be drawn by the author(s).

4. **COVERING LETTER:** All personal details, including name, year, name of college/university, postal address, phone number and e-mail id, must be provided in a separate letter or file, and must not be mentioned in the document or file containing the submission.

We encourage submission of contributions electronically. Kindly attach your contributions in MS Word format, mark the subject line of the email as **"CONTRIBUTION FOR NCU Law Review,"** and send it to **nculawreview@ncuindia.edu**. For any clarification, please write to us at the same email id.

THE NORTHCAP UNIVERSITY

Formerly ITM University, Gurugram

About the NorthCap University

Established in 1996 as ITM University, The NorthCap University is a leading multidisciplinary institution located in the heart of Gurugram, Haryana. With a rich legacy of over 30 years and a network of more than 15,000 alumni, the university has built strong connections with industry, government, and research organizations. Its modern urban campus hosts diverse schools offering programmes in law, engineering, technology, management, liberal arts, media, business, and applied sciences. Recognised by the UGC and the Bar Council of India, NCU is a member of AIU and ASQ and is accredited by ASIC, UK, as a Premier Institution. The university has earned a 5-Star rating in the QS Stars Rating System and ranks among India's top-performing universities in ARIIA. Accredited with NAAC Grade 'A', NCU promotes research, innovation, and industry engagement while providing global exposure through international partnerships, exchange programmes, dual degrees, and collaborative research opportunities.

About the School of Law

With the objective of providing students with ample scope of clinical legal education and assisting them in preparing for the future of law, the School of Law at The NorthCap University provides the highest quality of legal education. Students learn the skills necessary to be able to practice law transnationally and to cope with the new challenges and dimensions presented by the internationalisation of the legal profession. The school offers a comprehensive range of programmes, including the Five-Year Integrated BBA LL.B. (Hons.), Three-Year LL.B., LL.M., and Ph.D. in Law adhering to the following principles:

- Imbibing an Interdisciplinary Legal Approach to Education
- Introducing Innovations & Practicing in Real-Time
- Broadening Horizons for Quality Research

Conforming to the highest contemporary standards, the School of Law has shown all round progress and proved its credentials as a force to be reckoned with in the field of legal education in the country. With a commitment towards nation building through strong legal and ethical values, the school aims to advance political, social and economic justice and emerge as a preferred destination for students, faculty, employers and collaborators.

Key Highlights of NCU's School of Law

Industry Ready Curriculum: The course structure of the School of Law is regularly reviewed and updated to keep pace with fast-changing regulations, technology and skills, ensuring international competitiveness

Inter-disciplinary Approach in Law: The Integrated Programme provides students exposure to a wide range of courses having a combination of law, management, and technology, which enhances their employability skills

Choice-Based Electives: The school offers choice-based electives which help students specialize in their areas of interest

Foreign Languages: In addition to the regular course curriculum, students can learn various foreign languages. This increases a law graduate's ability to widen his/her horizon in the legal profession at a global level.

Teaching Pedagogy: Our students benefit from the use of modern audio-visual resources for classroom teaching, interactive sessions with experts, debates on current affairs, industry visits and more

A Competitive Moot Court Culture: Apart from maintaining a strong internal mooting structure, the Moot Court Society at NCU hosts an Annual National Moot Court Competition

Hands-on Training on Client Consultation: School of Law has imbibed an enriched culture of holding national client consultation competitions annually Technology Mediated Instruction: Blended learning experience through exposure to online MOOC courses and other online forums

Experienced Mentors: Expert faculty from reputed National Law Universities (NLUs) and Central Universities

Careers: Internship and placements support through the Centre for Professional Attachment & Alumni Engagement

THE NORTHCAP UNIVERSITY

Formerly ITM University, Gurugram

The NorthCap University, Gurugram
Tel.: +91-124-2365811 to 13 Email : law@ncuindia.edu
Website: www.ncuindia.edu

Printed and Published *by The NorthCap University (NCU), Gurugram and printed at Decorpac (I) Pvt. Ltd.,291 D, Sector 6, IMT Manesar, Distt. Gurugram - 122050 and published from The NorthCap University (NCU) Sector 23A, Gurugram - 122017, Haryana,* ***Editor-in-Chief*** *Prof. (Dr.) Archana Sarma*