About the Institute

IPEM made a modest beginning in the year 1996, with Management and Computer Application Programmes. Today the IPEM Group of Institutions is in the forefront of imparting knowledge in the fields of Law, Education, Management and Information Technology. The IPEM Law Academy is NAAC Accredited and Affiliated to Chaudhary Charan Singh University, Meerut and approved by the Bar Council of India. IPEM Law Academy offers LLM (2 YEARS), LL.B (3 years), B.A.LL.B (5 years) and B.Com LL.B (5 years) courses. The LLM (2 years) course was introuduced in 2024 with 20 seats. The LL.B (3 years) course was introduced in 2005 with 180 seats, B.A.LL.B (5 years) course was introduced in 2012 with 120 seats and B.Com LL.B (5 years) was introduced in 2019 with 60 seats. This is reflected in the performance of the Students as we have 100% result with maximum 1st. divisions. We provide the best placements to the students.

IPEM Law Academy has a spacious self contained campus spread across five acres of land. The infrastructure and layout of the Academy are planned in such a congenial manner that it is a learner's paradise.

In the course of their studies, the students are encouraged to visit the Parliament, the Supreme Court, High Courts and the District Courts; to participate in wide-ranging programs such as Seminars, Workshops, Symposiums, Conferences, Debates, Case Analysis Competitions, Guest Lectures and Moot courts. They are offered unique opportunity to put theory into practice by being a part of 'IPEM Legal Aid Clinic', the various Legal Aid Camps regularly organized by the institute, and Internship programmes.

Full encouragement is given to the students to become futuristic in their approach and endorse the quality of being 'Legal Professionals' of tomorrow. Students of Law are encouraged to pursue career options in various areas like Academics, Judicial Services, Advocacy, Law Consultancy, Law Officer, Legal Advisor, Armed Forces, Real Estate, and Legal Correspondents in Media or being placed in LPO / Law Firms. Besides these, Law graduates are considered more suitable and preferred by employers in other areas of employment also.

Located on NH-9 Bypass (Near Vijay Nagar, Ghaziabad), adjoining East Delhi, NOIDA & Greater Noida (West), the IPEM Law Academy is well connected by all modes of public transport also.

"Admission into professional course is not an achievement but an opportunity to hone one's professional skills and one must not let it pass by"
-Rephrased from the words of **Hon'ble Dr. Zakir Husain, former President of India**

Moot Court helps in learning what we learn in real courts although in restricted conditions. A Moot Court Competition simulates a court hearing (usually an appeal against a final decision), in which participants analyse a problem, research the relevant law, prepare written submissions, and present oral arguments. Moot court involves appellate cases as opposed to those at the trial level, which are often called "mock trials"; Judges are usually Law Professors, Advocates from the Community, and even members of the Judiciary.

The Legal Aid Clinic at IPEM Law Academy offers Students the opportunity to fine-tune their advocacy skills in a fast-paced, live-client setting by representing low-income clients under the careful guidance and thoughtful teaching of supervising Faculties and Advocates. The Legal Aid Clinic has been working to secure "Justice for and to Protect the Rights of the Needy". The Legal Aid Clinic faculty strives to select and assign cases that offer the greatest opportunity for impact and growth. Legal Aid Clinics are intended to provide Legal Relief which can be easily accessed by the 'indigent' and 'backward sections' of our society.

IPEM Law Academy employs highly interactive methodologies to teach students which include various Lecture Methodologies including, but not limited to, Lecture Method, Case Method, Problem Method, Discussion Method, Simulation and Role Play, Collaborative Teaching and Seminar Method. The plan on Teaching Methodologies also covers Lectures, Tutorial and Presentations.

A-13/1, South Side G.T. Road, Industrial Area, NH-24 By-Pass Ghaziabad, U.P. 201010
Email: info@ipemgzb.ac.in
Website: www.law.ipemgzb.ac.in
Telephone: 0120-4174500

IPEM LAW JOURNAL
Vol. 9 December 2025

ISSN 2581-3129
RNI No. UPBIL/2017/72947

IPEM LAW JOURNAL

The Annual Peer Reviewed and Refereed Journal of IPEM Law Academy

Vol. 9 December 2025

The Impact Of Cybersecurity And Data Protection Regulations On Startup Innovation And Performance: Evidence From Emerging Economies
Bouya Sara, El Kadiri Kenza

The Role Of Patent Law In Promoting Pharmaceutical Innovation: Ethical And Regulatory Perspectives
Dr. Vikas Sharma, Yuvraj Chhabra

Tech-driven Solutions To Global Death Penalty Challenges: Legislative And Judicial Approaches To Mandatory Capital Punishment In India And The USA
Swikriti Mahajan

Regulating Online Platform: Impact Of Online Harassment And Hate Speech On Women Participation In Political Activities
Alexander C., Dr. B. Venugopal

How AI Tools Challenge Traditional Methods Of Legal Interpretation: A Comparative Analysis With Indian Context
Dr. Pranav Ranga, Mr. Rahul Mehra

Re-Imagining Copyright Governance In India: Legal And Ethical Challenges In The Age Of Artificial Intelligence
Maitri Shail Patel, Dr. Sonal Raval

Balancing Privacy And Public Interest: The Emerging Landscape Of The Right To Be Forgotten In India
Junaid Malik

Guardians Of Data: From Brussels To Bharat
Anjali Aggarwal, Dr. Rahul Varshney

The Commons That Feed The Machines: Policy Reflections On Ai's Use Of Public Domain Works
K. Ankita Rao, Vishakha Sakharkar

Regulating Lantana Camara: A Legal Analysis With Special Reference To Deepor Beel In Assam
Dr. Gyanashree Dutta, Dr. Upankar Chutia

The Role Of AI Arti ficial Intelligence In The Consumer Protection Act of 2019
Mr. Mahesh S Betasur

Migration-related Vulnerabilities And Legal Safeguards For Women In Jammu & Kashmir
Ankita

डिजिटल निगरानी और निजता का अधिकार: राष्ट्रीय सुरक्षा एवं नागरिक स्वतंत्रताओं का संतुलन
डॉ योगेश कुमार गुप्ता

IPEM LAW ACADEMY
(ISO 9001:2015 Certified, NAAC ACCREDITED)

IPEM
LAW JOURNAL

Volume 9 December 2025 ISSN 2581-3129 (Print)

Patron
Mr. Anupam Goel
Secretary
Institute of Professional Excellence and Management, Ghaziabad, Uttar Pradesh

Mentor
Prof. (Dr.) Sugandha Goel
Executive Director
Institute of Professional Excellence and Management, Ghaziabad, Uttar Pradesh

Dr. Shashank Choudhary
Dean Academics
Institute of Professional Excellence and Management, Ghaziabad, Uttar Pradesh

Chief Editor
Prof. L. Pushpa Kumar
Professor, Faculty of Law
University of Delhi

Editorial Board
Dr. Tabrez Ahmad
Dean, GD Goenka University

Dr. G.B. Reddy
Professor, Osmania University, Hyderabad

Dr. Seema Singh
Associate Professor, Faculty of Law, University of Delhi

Dr. Digvijay Singh
Associate Professor, South Bihar Central University, Gaya

Dr. Sukhvinder
Assistant Professor, Dr. BR Ambedkar National Law University, Sonepat

Editorial Advisory Board
Dr. Vaibhav Goel Bhartiya
Dean, School of Law
Subharti University

Dr. Rama Sharma
Assistant Professor & HOD
Gautam Buddha University

Prof. Prasannanshu
Professor
NLU Delhi

Dr. Anupam Jha
Professor
University of Delhi

Prof. Sunanda Bharti
Professor
University of Delhi

Dr. Anjum Parvez
Associate Professor
Faculty of Law, Uttaranchal University

Dr. Lakshmi Priya Vinjamuri
Associate Professor
Faculty of Law, Uttaranchal University

Dr. Niteesh Kumar Upadhyay
Associate Professor
Symbiosis Law School, Noida

Dr. Abhinav Kumar Mishra
Adjunct Professor
Lloyd Law College, Greater Noida

Review Board
Prof. (Dr.) Mohd. Imran
Director, School of Law
Sushant University, Gurgaon

Dr. Sushim Shukla
Associate Professor
Tirthankar Mahavidyala, Muradabad

Dr. Vinod Kumar
Associate Professor
Amity University, Jaipur

Dr. Navtika Nautiyal
Assistant Professor
National Forensic Science University, Ahmedabad

Dr. Cholaraja Muddimannan
Assistant Professor
Faculty of Law, University of Delhi

Dr. Kavitha Chalakkal
Assistant Professor
Inter University Centre for IPR Studies, Cochin University

Ms. Deeksha Tiwari
Assistant Professor,
Amity Institute of Management and Law, Noida

Dr Rahul Mishra
Associate Professor & Head,
Legal Services Clinic,
Manipal Law School, Bangalor

Mr. Rachit Sharma
Assistant Professor,
IILM University, Greater Noida

Dr Pramod Tiwari
Sr. Assistant Professor,
Delhi University

Dr Purnima Chaudhary
HOD & Assistant Professor.
IPEM Law Academy, Ghaziabad

Ms. Sonam Singh
Assistant Professor.
IPEM Law Academy, Ghazaibad

Editor's Message

The Editorial Board of the IPEM Law Journal do hereby announce the publication of the ninth volume of its Journal. It is a matter of pride that the Journal is experiencing steady and healthy growth in circulation and readership. Research is an enduring field wherein persistent and focused efforts lead to positive results. All facets of the law are covered in the journal's articles. Contemporary advances are highlighted particularly, yet old topics are nonetheless given their proper respect and attention. The papers and articles published in the Journal are meant to appeal to a broad audience of anyone with an interest in the study of law, including professionals, academics, and students.

The Journal offers readers a chance to stay current on novel concepts and legal industry advances. The Evaluation Board, which is made up of impartial reviewers who serve as the Editorial Board, has received several research papers and articles for submission. Each manuscript has undergone a thorough review. We anticipate that the IPEM Law Journal will be a valuable resource for the legal community in terms of disseminating fresh perspectives and legal research. We thank everyone who has made a significant contribution to this Law Journal, especially the members of the Editorial Board for their tireless work. We also acknowledge the insightful suggestions and occasionally helpful advice from our Editorial Review Board. Finally, the members of the Editorial Board wish to thank the authors who submitted their papers and articles for the seventh issue of the Journal.

Any contributions in the form of research papers or articles are welcome for submission to the Editorial Board for the forthcoming issues of the Journal. Suggestions for improvement or otherwise in any part of the Journal are welcome and will be highly appreciated.

Chief Editor

Guidelines For Author's

1. Contributions should not exceed 5000 words including Charts, Tables and other Graphics.
2. The Research Paper should be preceded by an Abstract, not exceeding 150 words. 3. British spellings should be followed throughout (eg. programme, not program).
4. Tables and Charts should be in black & white only. These should be serially numbered sequentially. following references to them in the text and presented on separate sheets.
5. Two good Prints of the Article, in A-4 size stationary are required to be submitted. Matter should be formatted in Times New Roman, font size 12. The Title should be in upper case with font size 14. The main headings should be in upper case with font size 14 and subheadings should be formatted in lower case with font size 13. The manuscript should be clearly typed in double space with 1 and 1/2" wide margin on the left and 1/2" on the right side. The authors may note that the hard copy will be considered final and authentic.
6. Introduction and Conclusion must be added. This should be brief and state the relation with the present status of knowledge in the field.
7. All the Articles should be duly signed at the end.
8. Ciration in the text should simply give the name of the author and the year of publication quoted. For example: A.S. Agarwal (1970)
9. References should be given separately at the end of the paper and arranged alphabetically. The list should include only the work that the author's has cited.
10. References should include full details of the name(s) of the author(s), title of the article or book, name of the journal, details of the publishers, year & month of publication including page numbers, as appropriate. The following style should be strictly followed:
    a) **For Periodicals:** The author(s) name, year of publication, title of the article, journal name, volume and issue number and the page numbers of the article should be provided. For example: Mishra, K.M. (2002) Knowledge Management, New Delhi: Pearson Education MA: Allyn & Bacon,
    b) **For books:** Rowling. (2001) Harry Potter and the Sorcerer's Stone. London: Bloomsburg Children's.
    c) **For Magazine Article:** Kuliner, R. (2003, September 8) the great American pension-fund robbery, Business Week, 24-26,
    d) **If an article has no author, the periodical or newspaper is referenced as follows:** The Hindustan Times. (2008) RIL. finds new gas basin, November 27: 2010

e) **For unpublished works such as workings papers, dissertations and papers presentedat meetings, seminars, conferences etc:**

Tyagi, R.M, and Malik, S.P. (2007) Job Satisfaction Working Paper No 46, Indian Institute Of Travel Management, Gwalior Thakur, Reema, (2001) Effectiveness of different leadership styles on job satisfaction offactory workers. Unpublished doctoral dissertation. Jawahar Lal Nehru University, New Delhi

f) **For Article in Online Journal:** Jacoby, W. G. (1994). Public attitudes toward governmentspending. American Journal of Political Science, 38(2), 336-361. Retrieved fromhttp://www.jstor.org.

The Manuscript should be accompanied by:

1. A cover page containing the title, author's name &affiliation, mailing address, phone, fax number and e-mail address.
2. A second page containing the title, abstract summary (in about 150 words). In caseof multiple authors, the cover page should indicate the author to whom correspondence should be addressed to.
3. A declaration that the paper is original and has not been submitted/publishedelsewhere or presented.
4. Two passport photographs should be sent with brief resume

Note:

- Manuscripts not considered for publication will not be sent back. Acceptance of papersfor publication shall be informed through e-mail or through normal mail.
- Manuscripts that fail to conform to the guidelines will not be considered for publication.
- The ultimate decision to accept or reject a paper rest with the editorial board. The finaldraft of an accepted paper may be subjected to editorial amendments to suit the journal requirements.
- The author whose paper is published will receive one free copy of journal that carries thepaper.
- IPEM does not accept any responsibility for the views expressed in the articles by theauthors or for any inadvertent omissions. No part of the articles published in this JOURNAL should be reproduced without written permission from the Editor.

IPEM Law Journal

The Annual Referred Journal of Law of the Institute of Professional Excellence and Management

Vol. 9 December, 2025

Contents

The Impact Of Cybersecurity And Data Protection Regulations On Startup Innovation And Performance: Evidence From Emerging Economies 01
Bouya Sara, El Kadiri Kenza

The Role Of Patent Law In Promoting Pharmaceutical Innovation: Ethical And Regulatory Perspectives 06
Dr. Vikas Sharma, Yuvraj Chhabra

Tech-driven Solutions To Global Death Penalty Challenges: Legislative And Judicial Approaches To Mandatory Capital Punishment In India And The USA 14
Swikriti Mahajan

Regulating Online Platform: Impact Of Online Harassment And Hate Speech On Women Participation In Political Activities 27
Alexander C., Dr. B. Venugopal

How AI Tools Challenge Traditional Methods Of Legal Interpretation: A Comparative Analysis With Indian Context 36
Dr. Pranav Ranga, Mr. Rahul Mehra

Re-Imagining Copyright Governance In India: Legal And Ethical Challenges In The Age Of Artificial Intelligence 41
Maitri Shail Patel, Dr. Sonal Raval

Balancing Privacy And Public Interest: The Emerging Landscape Of The Right To Be Forgotten In India 56
Junaid Malik

Guardians Of Data: From Brussels To Bharat 69
Anjali Aggarwal, Dr. Rahul Varshney

The Commons That Feed The Machines: Policy Reflections On Ai's Use Of Public Domain Works 81
K. Ankita Rao, Vishakha Sakharkar

Regulating Lantana Camara: A Legal Analysis With Special Reference To Deepor Beel In Assam 94
Dr. Gyanashree Dutta, Dr. Upankar Chutia

The Role Of AI Arti ficial Intelligence In The Consumer Protection Act of 2019 105
Mr. Mahesh S Betasur

Migration-related Vulnerabilities And Legal Safeguards For Women In Jammu & Kashmir 112
Ankita

डिजिटल निगरानी और निजता का अधिकार: राष्ट्रीय सुरक्षा एवं नागरिक स्वतंत्रताओं का संतुलन 124
डॉ योगेश कुमार गुप्ता

THE IMPACT OF CYBERSECURITY AND DATA PROTECTION REGULATIONS ON STARTUP INNOVATION AND PERFORMANCE: EVIDENCE FROM EMERGING ECONOMIES

EL Kadiri Kenza[1]
Bouya Sara[2]

ABSTRACT

The growing wave of cybersecurity and data protection regulations is reshaping entrepreneurial ecosystems in emerging economies (Goldfarb & Tucker, 2011; European Parliament, 2016). This paper examines how such regulations influence startup innovation and performance by combining insights from the resource-based view (Barney, 1991), dynamic capabilities (Teece, 2007), and institutional theory (DiMaggio & Powell, 1983). Using a conceptual framework and an empirical strategy based on firm-level panel data (Cohen & Levinthal, 1990; Khanna & Palepu, 2010), the study finds that while compliance initially constrains innovation due to costs and complexity, it later enhances strategic innovation quality and customer trust, leading to superior performance (Porter & van der Linde, 1995; Goldfarb & Tucker, 2011). The findings offer implications for startup founders, investors, and policymakers seeking to balance regulatory enforcement with innovation-driven growth in dynamic and resource-constrained environments (La Porta et al., 1998; Blind, 2012).

Keywords: *cybersecurity, data protection, startups, innovation, emerging economies, regulation.*

I. INTRODUCTION

Digital transformation has accelerated data collection and processing in emerging economies, increasing both the opportunities and vulnerabilities for startups (Brynjolfsson & McAfee, 2014; Kshetri, 2013). Governments have responded by adopting cybersecurity and data protection frameworks inspired by the EU's GDPR (European Parliament, 2016) and adapted to local contexts (Khanna & Palepu, 2010). Yet, a fundamental tension persists: do these regulations inhibit innovation by imposing compliance costs, or do they foster trust and competitiveness by establishing secure digital environments? (Porter & van der Linde, 1995; Goldfarb & Tucker, 2011). This question is particularly relevant in emerging economies, where institutional weaknesses and limited financial resources amplify regulatory impacts (Cohen & Levinthal, 1990; Teece, 2007).

2. RESEARCH PROBLEM AND CONTRIBUTION

Existing research often treats regulatory burdens (Bessen & Meurer, 2008) and consumer trust mechanisms (Pavlou & Gefen, 2004) separately, overlooking how they interact in startup ecosystems of emerging economies (Khanna & Palepu, 2010; La Porta et al., 1998). This paper contributes by (1) proposing a hybrid framework integrating resource-based, dynamic, and institutional perspectives (Barney, 1991; Teece, 2007; DiMaggio & Powell, 1983), (2) developing testable hypotheses on the short- and medium-term impacts of data protection regulations on innovation

[1]*Research Professor, Laboratory of Economic Sciences and Public Policies (LSEPP), Department of Economics, Faculty of Economics and Management, Ibn Tofail University, Kenitra, Morocco (kenza.elkadiri@uit.ac.ma)*
[2]*Doctoral Student, Laboratory of Economic Sciences and Public Policies (LSEPP), Department of Economics, Faculty of Economics and Management, Ibn Tofail University, Kenitra, Morocco (sarra.bouya@uit.ac.ma)*

and performance (Blind, 2012; Porter & van der Linde, 1995), and (3) outlining a robust empirical strategy using firm-level panel data from multiple emerging economies (World Bank, 2019; Acemoglu & Robinson, 2012).

3. LITERATURE REVIEW

3.1 CYBERSECURITY AND DATA PROTECTION REGULATIONS

The relationship between regulation and innovation is multidimensional. While the "Porter Hypothesis" argues that well-designed regulations can enhance competitiveness by stimulating innovation (Porter & van der Linde, 1995), other studies highlight compliance costs and reduced flexibility, especially for small firms (Bessen & Meurer, 2008; Blind, 2012). Data protection frameworks such as the GDPR impose security, consent, and reporting requirements that reshape business models and data monetization strategies (European Parliament, 2016; Goldfarb & Tucker, 2011). The economics of information security literature further links compliance to risk mitigation and consumer trust (Anderson & Moore, 2006; Kshetri, 2013).

3.2 STARTUP INNOVATION AND REGULATORY CONSTRAINTS

Startups rely on scarce resources, agility, and learning capabilities to innovate (Barney, 1991; Cohen & Levinthal, 1990). Compliance obligations, however, redirect resources from R&D toward legal and technical adjustments (Bessen & Meurer, 2008). Nonetheless, early compliance can build legitimacy and differentiation, turning security and privacy into competitive assets (Pavlou & Gefen, 2004; Brynjolfsson & McAfee, 2014). Studies on architectural innovation emphasize that startups adapt existing technologies to meet new regulatory environments (Henderson & Clark, 1990; West & Bogers, 2014).

3.3 THE CONTEXT OF EMERGING ECONOMIES

Institutional quality, legal enforcement, and market maturity moderate the relationship between regulation and performance (La Porta et al., 1998; Acemoglu & Robinson, 2012). In emerging economies, weak enforcement and limited technical capacity make regulatory compliance disproportionately costly for startups (Khanna & Palepu, 2010; Kshetri, 2013). However, these same environments provide opportunities for leapfrogging through digital trust innovation (Lee & Trimi, 2018; Prahalad & Hammond, 2002).

4. THEORETICAL FRAMEWORK AND HYPOTHESES

This study integrates three perspectives.

Resource-Based View (RBV): cybersecurity and data governance capabilities are strategic resources generating sustainable competitive advantage (Barney, 1991).

Dynamic Capabilities Theory: startups can adapt and reconfigure these resources in response to regulatory shocks (Teece, 2007).

Institutional Theory: regulatory harmonization and mimetic pressures shape firm behavior across sectors (DiMaggio & Powell, 1983).

Hypotheses:

H1: The introduction or tightening of data protection regulations negatively affects startup innovation in the short term (Bessen & Meurer, 2008; Goldfarb & Tucker, 2011).

H2: In the medium term, compliance fosters higher

innovation quality and trust-based performance improvements (Pavlou & Gefen, 2004; Porter & van der Linde, 1995).

H3: These effects are moderated by absorptive capacity (Cohen & Levinthal, 1990), access to finance (Khanna & Palepu, 2010), and institutional enforcement (La Porta et al., 1998).

5. EMPIRICAL STRATEGY AND METHODOLOGY

5.1 DATA

The empirical strategy proposes a multi-country panel dataset combining:

World Bank Enterprise Surveys (WBES) for firm-level innovation and performance indicators (World Bank, 2019),

Regulatory databases tracking data protection and cybersecurity laws (European Parliament, 2016), and

Startup financing data from Crunchbase and PitchBook (Khanna & Palepu, 2010).

5.2 VARIABLES

Dependent Variables: innovation (R&D expenditure, new products, patents) and performance (revenue growth, funding, survival) (Arora, Fosfuri, & Gambardella, 2001; Barney, 1991).

Independent Variables: regulatory exposure (pre/post implementation), regulatory stringency, compliance cost.

Moderators: firm size, age, financing access, absorptive capacity, institutional quality (Cohen & Levinthal, 1990; La Porta et al., 1998).

5.3 ECONOMETRIC MODEL

A difference-in-differences (DiD) approach with firm and year fixed effects is used to estimate the causal impact of regulation on innovation and performance, controlling for country-specific trends (Angrist & Pischke framework implied). Robustness checks include instrumental variables (e.g., regional harmonization), Probit/Logit models for financing probability, and event-study estimations (Teece, 2007; Cohen & Levinthal, 1990).

6. EXPECTED RESULTS AND INTERPRETATION

Building on prior studies (Porter & van der Linde, 1995; Goldfarb & Tucker, 2011; Bessen & Meurer, 2008), we expect:

Short-term decline in innovation due to compliance costs.

Medium-term gains through innovation reorientation toward security and trustworthiness (Henderson & Clark, 1990; Pavlou & Gefen, 2004).

Heterogeneous effects: smaller, underfunded startups face constraints, while those with strong absorptive capacity and external funding benefit more (Cohen & Levinthal, 1990; Khanna & Palepu, 2010).

7. DISCUSSION AND MANAGERIAL IMPLICATIONS

Policymakers should provide targeted support (training, subsidies, and simplified compliance) to reduce the regulatory burden on startups (Blind, 2012; Khanna & Palepu, 2010). Entrepreneurs should view compliance not as a constraint but as a trust-building opportunity that enhances credibility and market access (Pavlou & Gefen, 2004; Brynjolfsson & McAfee, 2014). At the macro level, regulatory harmonization across regions can lower transaction costs and foster innovation diffusion (European Parliament, 2016; La Porta et al., 1998).

8. LIMITATIONS AND FUTURE RESEARCH

This study's main limitation is data availability and comparability of innovation measures across startups

(Arora et al., 2001; Henderson & Clark, 1990). Future research could:

Conduct **qualitative studies** (interviews, case studies) on startup adaptation strategies (Cohen & Levinthal, 1990).

Analyze **cross-country regulation timing** for stronger causal inference.

Examine **sectoral differences,** such as fintech and healthcare (Goldfarb & Tucker, 2011; Kshetri, 2013).

9. CONCLUSION

Cybersecurity and data protection regulations in emerging economies represent both a **challenge and an opportunity** for startups (Goldfarb & Tucker, 2011; European Parliament, 2016). Our analysis suggests a two-phase effect: initial constraints on innovation followed by improved performance once trust and legitimacy are established (Barney, 1991; Teece, 2007). Policymakers and entrepreneurs must therefore co-design ecosystems where regulation acts as a catalyst for sustainable innovation and competitiveness (Porter & van der Linde, 1995; Khanna & Palepu, 2010).

REFERENCES

1. Acemoglu, D., & Robinson, J. A. (2012). Why nations fail: The origins of power, prosperity, and poverty. Crown.

2. Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610–613.

3. Arora, A., Fosfuri, A., & Gambardella, A. (2001). Markets for technology: The economics of innovation and corporate strategy. MIT Press.

4. Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120.

5. Benkler, Y. (2006). The wealth of networks: How social production transforms markets and freedom. Yale University Press.

6. Bessen, J., & Meurer, M. J. (2008). Patent failure: How judges, bureaucrats, and lawyers put innovators at risk. Princeton University Press.

7. Blind, K. (2012). The influence of regulations on innovation: A framework and review. In Handbook of the Economics of Innovation (Eds. Hall & Rosenberg).

8. Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton & Company.

9. Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. Administrative Science Quarterly, 35(1), 128–152.

10. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160.

11. European Parliament. (2016). Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR). Official Journal of the European Union.

12. Goldfarb, A., & Tucker, C. (2011). Privacy regulation and online advertising. Management Science, 57(1), 57–71.

13. Henderson, R. M., & Clark, K. B. (1990). Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms. Administrative Science Quarterly, 35(1), 9–30.

14. Khanna, T., & Palepu, K. (2010). Winning in emerging markets: A road map for strategy and execution. Harvard Business Review Press.

15. Kshetri, N. (2013). Cybercrime and cybersecurity in

the global south. Third World Quarterly, 34(1), 114–132.

16. La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. (1998). Law and finance. Journal of Political Economy, 106(6), 1113–1155.

17. Lee, S. M., & Trimi, S. (2018). Innovation for creating a smart future. Journal of Open Innovation: Technology, Market, and Complexity, 4(4), 50.

18. Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. Information Systems Research, 15(1), 37–59.

19. Porter, M. E., & Stern, S. (2001). Innovation: Location matters. MIT Sloan Management Review, 42(4), 28–36.

20. Porter, M. E., & van der Linde, C. (1995). Toward a new conception of the environment-competitiveness relationship. Journal of Economic Perspectives, 9(4), 97–118.

21. Prahalad, C. K., & Hammond, A. (2002). Serving the world's poor, profitably. Harvard Business Review, 80(9), 48–57.

22. Purdy, G., & Daugherty, P. (2017). How AI boosts industry profits and innovation. Harvard Business Review.

23. Schumpeter, J. A. (1942). Capitalism, socialism and democracy. Harper & Brothers.

24. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319–1350.

25. Verizon. (2019). Data breach investigations report. Verizon.

26. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144.

27. West, J., & Bogers, M. (2014). Leveraging external sources of innovation: A review of research on open innovation. Journal of Product Innovation Management, 31(4), 814–831.

28. World Bank. (2019). Enterprise Surveys: Firm-level data on business environment and performance. The World Bank Group.

29. Zhang, X., & Zhu, F. (2019). Does privacy regulation hinder innovation? Evidence from mobile apps. Management Science, 65(5), 2253–2276.

THE ROLE OF PATENT LAW IN PROMOTING PHARMACEUTICAL INNOVATION: ETHICAL AND REGULATORY PERSPECTIVES

Dr Vikas Sharma[1]
Yuvraj Chhabra[2]

ABSTRACT

Patent law serves as a critical mechanism in fostering innovation within the pharmaceutical industry by granting inventors exclusive rights to their discoveries for a limited period. This legal protection encourages substantial investment in research and development (R&D), as pharmaceutical companies can anticipate a return on their investment through market exclusivity. The industry, characterized by high development costs, lengthy clinical trials, and stringent regulatory approval processes, relies heavily on patent protection to sustain innovation and competitiveness.However, the intersection of patent law with ethics raises significant questions. While patents incentivize innovation, they can also create barriers to access, particularly for essential medicines in low- and middle-income countries. Ethical debates center on balancing the need to reward innovation with the moral imperative of ensuring public health and equitable access to life-saving drugs. Regulatory frameworks, including international agreements such as the TRIPS (Trade-Related Aspects of Intellectual Property Rights), aim to harmonize patent protection while allowing flexibilities such as compulsory licensing during public health emergencies. This study explores the multifaceted impact of patent law on pharmaceutical innovation, examining how legal frameworks influence research priorities, technology transfer, and ethical considerations. It analyzes the effectiveness of existing regulations in promoting both innovation and accessibility, highlighting challenges faced by policymakers, regulators, and the pharmaceutical industry. By evaluating the ethical, legal, and technological dimensions, this research seeks to provide insights into creating a balanced system that incentivizes innovation while safeguarding public health interests.The findings of this study are expected to contribute to policy recommendations for refining patent laws and regulatory practices, ensuring that they foster sustainable innovation in the pharmaceutical sector without compromising ethical and social responsibilities.

Keywords: *Patent Law, Pharmaceutical Innovation, Ethics in Healthcare, Regulatory Frameworks, Access to Medicines*

I. INTRODUCTION

Pharmaceutical innovation plays a crucial role in improving global health outcomes by developing new drugs and therapies for diseases that were previously untreatable. However, the development of pharmaceuticals is inherently risky, time-consuming, and expensive, often requiring years of research, clinical trials, and regulatory approval. In this context, patent law serves as a critical mechanism for incentivizing innovation by granting inventors temporary exclusive rights to their discoveries. These rights allow pharmaceutical companies to recoup their investment costs and profit from novel drugs, thereby encouraging continued research and development.

[1]*Associate Professor, Institute of Legal Studies and Research, Faculty of law, Mangalayatan University, Aligarh, UP, India*

[2]*Research Scholar, Institute of Legal Studies and Research, Faculty of law, Mangalayatan University, Aligarh, UP, India*

The ethical dimension of patent law emerges when considering access to essential medicines. While patents promote innovation, they can also lead to high drug prices, creating barriers for low-income populations and exacerbating global health disparities. This tension between incentivizing innovation and ensuring equitable access raises important questions about the moral responsibilities of pharmaceutical companies, policymakers, and the global community.

Regulatory frameworks complement patent protection by establishing standards for drug approval, safety, and efficacy, thereby fostering trust in new therapies. International agreements, such as the Trade-Related Aspects of Intellectual Property Rights (TRIPS), further shape the global pharmaceutical landscape by standardizing patent protections while allowing for mechanisms like compulsory licensing to balance public health needs.

This paper examines the dual role of patent law in the pharmaceutical industry: as a driver of innovation and as a source of ethical debate. By analyzing regulatory frameworks, ethical considerations, and case studies, the study aims to provide a comprehensive understanding of how patent law can both encourage the development of life-saving medicines and simultaneously create challenges for equitable access. The findings will inform policy suggestions to optimize innovation while upholding ethical obligations toward public health.

II. OBJECTIVES OF THE STUDY

1. To examine the role of patent law in incentivizing pharmaceutical research and innovation.
2. To analyze the ethical implications of patent protection in the pharmaceutical industry, especially regarding access to essential medicines.
3. To evaluate regulatory frameworks, including international treaties and national laws, in balancing innovation incentives and public health needs.
4. To propose strategies for harmonizing patent protection with ethical and social responsibilities in pharmaceutical innovation.

III. RESEARCH METHODOLOGY

This study employs a qualitative research methodology to examine the role of patent law in pharmaceutical innovation and its ethical implications. Primary sources include international patent regulations, World Health Organization (WHO) reports, and legal frameworks such as TRIPS. Secondary sources consist of academic articles, case studies, and industry reports that analyze the impact of patents on drug development, pricing, and accessibility. A comparative approach is used to assess how different countries implement patent laws and manage public health needs. Ethical analysis is conducted using normative frameworks, such as utilitarianism and human rights principles, to evaluate the societal consequences of patent protections. Data collection focuses on real-world examples of patented drugs, access challenges in developing countries, and regulatory interventions such as compulsory licensing. The methodology allows for a holistic understanding of both the legal incentives for innovation and the ethical dilemmas arising from restricted access to essential medicines.

IV. THE ROLE OF PATENT LAW IN PROMOTING PHARMACEUTICAL INNOVATION

Patent law has significantly influenced pharmaceutical innovation by providing exclusive rights that encourage investment in research and development.

Companies can recover the high costs associated with drug discovery, clinical trials, and regulatory approval, which would otherwise deter innovation. This protection fosters competition and incentivizes the creation of novel therapies, particularly in areas of high unmet medical need.

However, these benefits come with ethical challenges. Patents can limit access to essential medicines, especially in low-income countries, by allowing high pricing. Regulatory measures, including compulsory licensing and tiered pricing models, attempt to mitigate these effects while preserving incentives for innovation. Case studies in HIV/AIDS and COVID-19 therapeutics illustrate the tension between encouraging pharmaceutical progress and ensuring equitable access. The interplay between patent protection, regulation, and ethics highlights the need for balanced policies that promote innovation without compromising public health priorities.

1. The role of patent law in incentivizing pharmaceutical research and innovation

Patent law plays a fundamental role in shaping the landscape of pharmaceutical research and innovation by providing companies with a temporary monopoly over their inventions. This exclusive right, typically lasting 20 years from the filing date, allows pharmaceutical firms to commercialize new drugs without competition from generic manufacturers. Since drug development is a long, expensive, and high-risk process, patents serve as a crucial incentive for companies to invest substantial resources into research and development (R&D).

Bringing a new drug to market can cost billions of dollars and may take more than a decade of research, clinical trials, and regulatory approval processes. Many potential compounds fail during testing, meaning the financial risk for pharmaceutical companies is significant. Patent protection helps justify this investment by giving innovators a period in which they can charge higher prices to recoup costs and generate profit, which in turn funds further innovation. Without such protection, competitors could easily replicate a drug once it is discovered, undermining the innovator's ability to recover their investment.

In addition to financial protection, patents encourage knowledge sharing. To obtain a patent, inventors must fully disclose their invention, which contributes to scientific understanding and may spark further innovation by other researchers. This disclosure ensures that once the patent expires, the public gains access to detailed information about the drug's formulation and production, paving the way for affordable generics.

Patent law also stimulates competition among pharmaceutical companies to discover novel and more effective therapies. Firms are motivated to innovate in order to secure exclusive rights, leading to a continuous cycle of research and advancement in medical science. Breakthroughs in areas such as cancer, HIV/AIDS, and rare diseases often emerge from the competitive environment fostered by patent incentives.

Despite criticisms, particularly regarding high drug prices during patent periods, the system remains an essential mechanism for promoting pharmaceutical innovation. Policymakers attempt to balance the interests of innovators and consumers with complementary measures such as patent term adjustments, regulatory exclusivities, and incentives

for orphan drugs. Ultimately, while not perfect, patent law remains a cornerstone of the pharmaceutical industry, driving scientific progress and enabling the development of life-saving and life-improving medicines.

2. Ethical implications of patent protection in the pharmaceutical industry, especially regarding access to essential medicines

While patent protection plays an important role in incentivizing pharmaceutical innovation, it also presents significant ethical challenges, particularly in relation to access to essential medicines. The ethical debate centers on the conflict between intellectual property rights—which reward innovation—and the moral obligation to ensure that life-saving medicines are available and affordable to all.

One major ethical concern is that patents allow companies to set high prices for new drugs, often placing them beyond the reach of low-income populations and even straining healthcare systems in wealthier nations. When medicines for diseases such as HIV/AIDS, tuberculosis, cancer, or diabetes are priced too high, the result can be preventable suffering and deaths. This raises profound ethical questions about prioritizing profit over human life and public health.

Equity is another central issue. Patent rules, particularly under international agreements such as TRIPS (Trade-Related Aspects of Intellectual Property Rights), can disproportionately affect developing countries, where the burden of disease is often greatest and financial resources are limited. Ensuring that all people have access to essential medicines, regardless of their socioeconomic status or geographic location, is widely recognized as a fundamental component of global health justice.

Ethical frameworks such as utilitarianism and human rights perspectives further illuminate the problem. From a utilitarian standpoint, denying access to medicine reduces overall societal well-being. From a human rights perspective, access to essential medicines is directly linked to the right to health. When patent protection restricts this access, it becomes ethically problematic.

Pharmaceutical companies argue that without patent protection, innovation would stagnate, leaving future patients without new treatments. While this has some validity, critics stress the need for a balance. Alternative models—such as compulsory licensing, patent pools, tiered pricing, public-private partnerships, and government-funded research—are often proposed to reconcile innovation incentives with ethical obligations.

The COVID-19 pandemic brought these issues into sharp focus, highlighting global disparities in vaccine access. It sparked debate about whether waiving patent protections for emergency medicines is morally necessary during global crises.

In conclusion, while patent protection is vital for encouraging innovation, it poses ethical challenges regarding equity, affordability, and the universal right to health. Addressing these concerns requires a nuanced and collaborative approach that balances the interests of innovators with the moral imperative to ensure that essential medicines are accessible to all.

3. Evaluating Regulatory Frameworks in Balancing Innovation Incentives and Public Health Needs

Regulatory frameworks—including international treaties, national patent laws, and public health

policies—play a central role in mediating the tension between incentivizing pharmaceutical innovation and ensuring equitable access to medicines. International agreements such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) establish baseline global standards for patent protection, granting pharmaceutical innovators exclusive rights for typically 20 years. These protections encourage investment in high-risk, high-cost research by allowing innovators to recoup development expenditures and earn profits. However, the same exclusivity can limit affordability and access, especially in low- and middle-income countries (LMICs).

To address these challenges, TRIPS includes flexibilities such as compulsory licensing, parallel importation, and provisions for public health emergencies. These mechanisms allow governments to override patent protection under specific conditions to ensure access to essential medicines. The Doha Declaration further reaffirmed that public health concerns take precedence over trade rules, enabling countries to use TRIPS flexibilities without violating international obligations. Despite this, LMICs often struggle to utilize these tools due to political pressure, lack of administrative capacity, and fear of trade retaliation.

National laws further shape the balance between innovation and access. Many high-income countries implement regulatory exclusivities—such as data exclusivity, market exclusivity for orphan drugs, and patent term extensions—designed to supplement traditional patents. While these measures promote innovation in areas like rare diseases and biologics, they can prolong monopolies and delay the entry of generics and biosimilars.

Regulatory agencies such as the FDA and EMA contribute by ensuring that approved drugs meet safety and efficacy standards, but they also influence innovation through incentives like priority review vouchers and accelerated approval pathways. These incentives aim to guide research toward unmet medical needs, though critics argue they may be misused or insufficient in addressing global health priorities.

Overall, regulatory frameworks attempt to strike a balance between fostering innovation and safeguarding public health, but the equilibrium remains imperfect. Effective policy requires dynamic, context-sensitive governance that recognizes both the economic realities of drug development and the moral imperative of universal access.

4. Strategies for Harmonizing Patent Protection with Ethical and Social Responsibilities in Pharmaceutical Innovation

Achieving harmony between strong patent protection and ethical obligations to ensure global access to medicines requires adopting multifaceted strategies that support innovation while upholding social justice. One foundational approach is reforming patent systems to prioritize genuine innovation over incremental changes. Strengthening examination standards to prevent "evergreening"—the practice of extending patent life through minor modifications—can prevent unnecessary monopolies and accelerate the availability of generics.

Another strategy involves expanding the use of differential pricing. Under this model, pharmaceutical companies set drug prices based on a country's income

level and ability to pay. This enables access in LMICs while allowing manufacturers to maintain profits in high-income markets. Transparency in pricing mechanisms, along with international cooperation, can prevent arbitrage and maintain market integrity.

Voluntary licensing and patent pooling also offer powerful tools. Through mechanisms such as the Medicines Patent Pool (MPP), patent holders can license their innovations to qualified manufacturers under agreed terms. This enables broader, cost-effective production while ensuring that innovators receive royalties. Public–private partnerships, especially in neglected-disease research, can further align commercial incentives with societal needs by sharing costs, risks, and benefits.

Governments can also promote ethical innovation by conditioning public research funding on access-oriented requirements. For example, institutions receiving public funds may be required to adopt socially responsible licensing terms that prioritize affordability in low-income settings. Similarly, transparency in R&D costs can inform more equitable pricing and strengthen public trust.

Global frameworks should also be strengthened. Clarifying the implementation of TRIPS flexibilities, providing technical assistance to LMICs, and promoting international cooperation during health crises can ensure that patent rights do not impede access to essential medicines. Ethical review bodies can incorporate social-impact assessments into drug development evaluations, ensuring that decisions reflect broader societal considerations rather than purely commercial factors.

Lastly, promoting alternative incentive structures—such as prize funds, advance market commitments, and delinkage models—can reward innovation without relying solely on high drug prices derived from monopoly protection. These models can be particularly effective in stimulating research in areas with limited commercial appeal, such as antimicrobial resistance and neglected tropical diseases.

In sum, harmonizing patent protection with ethical responsibilities requires a balanced mix of legal reforms, cooperative mechanisms, transparent pricing, and innovative incentive systems that collectively support both scientific progress and global health equity.

V. SUGGESTION AND CONCLUSION

To balance pharmaceutical innovation with equitable access, several policy and regulatory strategies can be implemented. First, governments can encourage public-private partnerships to share the financial risks of drug development, reducing reliance on high drug prices to recoup costs. This model can also promote research in neglected diseases that are often less profitable.

Second, compulsory licensing provisions should be streamlined and more widely used in emergencies, allowing countries to produce or import generic versions of essential medicines without violating patent rights. This ensures life-saving treatments are accessible during health crises, while still respecting international IP agreements.

Third, tiered pricing and differential pricing strategies can help make patented drugs affordable for low- and middle-income populations. Pharmaceutical companies could adopt voluntary licensing agreements with generic manufacturers to expand

access in resource-limited regions.

Fourth, governments and international organizations can provide incentives for innovation beyond patents, such as research grants, tax credits, and prize funds for breakthrough therapies. These measures reduce over-reliance on monopolistic pricing as the primary incentive.

Lastly, transparent collaboration between pharmaceutical firms, regulators, and global health agencies can align incentives with ethical imperatives. By integrating innovation-driven policies with mechanisms that ensure access, it is possible to foster a pharmaceutical ecosystem that both advances science and addresses public health equity.

CONCLUSION

Patent law plays a dual role in the pharmaceutical industry, simultaneously promoting innovation and presenting ethical challenges. By granting temporary monopolies on new drugs, patents incentivize companies to invest in costly and high-risk research and development. This protection has led to significant medical breakthroughs, including treatments for cancer, HIV/AIDS, and rare diseases, ultimately improving global health outcomes. Patent law also encourages knowledge sharing, as inventors must disclose their innovations, which benefits future research once patents expire.

However, these benefits are accompanied by ethical concerns related to access and affordability. High prices for patented medicines can limit availability in low-income regions, creating disparities in health outcomes and raising questions about the moral responsibilities of pharmaceutical companies and policymakers. International agreements like TRIPS attempt to balance innovation incentives with public health needs, but tensions remain. Regulatory tools such as compulsory licensing, differential pricing, and public-private partnerships can mitigate these ethical challenges, providing a pathway to equitable access while maintaining innovation incentives.

In conclusion, patent law is indispensable for advancing pharmaceutical research, yet its implementation must be guided by ethical considerations and regulatory oversight. Achieving a balance between incentivizing innovation and ensuring global access to essential medicines requires coordinated efforts among governments, industry, and international organizations. With thoughtful policies, it is possible to foster a pharmaceutical landscape that drives scientific progress while upholding the principles of equity, justice, and public health.

REFERENCES

1. Akinsolu, F. T., de Paiva, V. N., Souza, S. S., & colleagues. (2017). Patent landscape of neglected tropical diseases: An analysis of worldwide patent families. Globalization and Health, 13, Article 82. https://doi.org/10.1186/s12992-017-0306-9 BioMed Central

2. Ferpozzi, H. (2023). Public private partnerships and the landscape of neglected tropical disease research: The shifting logic and spaces of knowledge production. Minerva. Advance online publication. https://doi.org/10.1007/s11024-023-09496-x PMC+1

3. Ma, Z., Augustijn, K., De Esch, I., & Bossink, B. (2023). Public private partnerships influencing the initiation and duration of clinical trials for neglected tropical diseases. PLOS Neglected Tropical Diseases, 17(11), e0011760. https://doi.org/10.1371/journal.pntd.

0011760 PMC

4. Liese, B. H., Houghton, N., & Teplitskaya, L. (2014). Progress in public–private partnerships to fight neglected diseases. International Health, 6(3), 162–171. https://doi.org/10.1093/inthealth/ihu052 PubMed

5. Louët, S. (2003). Public–private partnerships boost research on neglected diseases. Nature Biotechnology, 21(11), 1254–1255. https://doi.org/10.1038/nbt903 PMC

6. de Vrueh, R. L. A., & de Vlieger, J. S. B. (2019). Public private partnerships as drivers of innovation in healthcare. Frontiers in Medicine, 6, article 114. https://doi.org/10.3389/fmed.2019.00114 frontiersin.org

7. Poynton, A. S. (2024). The incentive argument in pharmaceutical patent law. Journal of Global Trade, Ethics and Law, 1(4), 1–23. https://doi.org /10.5281/zenodo.10529407 journalgtel.com

8. Hussain, M., & others. (2024). Patents and public health: State responsibility to opt for a balanced approach. Societies, 14(8), Article 152. https://doi.org/10.3390/soc14080152 MDPI

9. Khan, M. D., Habib, R. I., Ahmad, R. N., & Safdar, A. (2020). Role of the Medicine Patent Pool (MPP) in resolving conflict between patents and access to essential medicines. European Online Journal of Natural and Social Sciences, 9(3), 601–609. European Science

10. Watal, J. (WTO). (n.d.). Implementation of paragraph 6 of the Doha Declaration on the TRIPS Agreement and public health. In WTO TRIPS and Public Health documentation. World Trade Organization. Retrieved from https://www.wto.org/ english/tratop_e/trips_e/implem_para6_e.htm World Trade Organization innovation. Journal of Product Innovation Management, 31(4), 814–831.

28. World Bank. (2019). Enterprise Surveys: Firm-level data on business environment and performance. The World Bank Group.

29. Zhang, X., & Zhu, F. (2019). Does privacy regulation hinder innovation? Evidence from mobile apps. Management Science, 65(5), 2253–2276.

TECH-DRIVEN SOLUTIONS TO GLOBAL DEATH PENALTY CHALLENGES: LEGISLATIVE AND JUDICIAL APPROACHES TO MANDATORY CAPITAL PUNISHMENT IN INDIA AND THE USA

Swikriti Mahajan[1]

ABSTRACT

The global debate concerning the death penalty has also entered a new phase of changes due to the fact that the law regimes touch upon the increasing influence of the technology on the criminal justice process. The next research article discusses how technological solutions, such as digital evidence solutions and forensic innovations, and their analysis solutions on algorithmic risk-assessment are changing the legislative and judicial reaction to the compulsory capital punishment in India and the United States. Common constitutional commitments to due process and human dignity exist between the two jurisdictions but the statutory framework, institutional protection and sentencing for each differ significantly.

The paper starts by bringing the criminal nature of the mandatory death penalty regimes to the fore issue of human rights in the world through observing that the international world is increasingly getting convinced that compulsory capital punishment structures are not relevant to the shifting requirements of decency. It is against this background that the paper analyses the way in which courts and legislatures in both India and USA are integrating the application of technological interviewing to reduce wrongful conviction, provide individualized sentencing and procedural fairness. Of the most significant innovations, including digital chain-of-custody, AI-assisted-forensic-analysis, electronic case-management, and predictive analytics, are of most importance, assessed critically in terms of their abilities to improve the evidentiary reliability of capital cases.

It has also been seen through the comparative analysis that there are big challenges. There exists a threat of algorithmic instruments that are loaded with race, caste, or socio-economic bias; digital evidence is dubbed in significance of authenticity and manipulation; and absence of fundamental access to the forensic instruments of high tech can contribute to the state of injustice. The article evaluates how the Indian courts after the doctrine of the rarest of rare and the U.S. courts after the landmark jurisprudence of Eighth and Fourteenth Amendments are grappling with such complexities in undertaking the review of the death-qualified offences and the sentencing processes.

Lastly, paper believes that, despite the meaning those technology is to be used as a means of fostering fairness, transparency, and individualized justice, it cannot replace the powerful constitutional checking or moral safeguards. The USA and India need to accept moderate and humanistic solutions that will not lead to the compromise of due process, judicial independence and the need to protect wrongful executions by adopting technological advances.

Keywords: *Mandatory death penalty; capital punishment; India; the United States; technology in criminal justice; digital evidence; forensic technology; algorithmic decision-making; individualized sentencing; comparative criminal law.*

[1]*PHD Scholar University of Jammu*

I. INTRODUCTION

Capital punishment remains one of the most debatable phenomena in the context of global criminal justice, especially at the time when countries have to face the ethical, procedural, and technological dilemma of the death penalty. The world over in the recent years has shifted to rights-based constitutionalism and due-process norms, which has pressured courts and legislatures to reconsider not only the substantive foundation of capital punishment, but the procedures of imposing death sentences. This reevaluation is further complicated in the jurisdictions where the law requires the death penalty to be made in particular offences, restricting the power of the judge and bringing up the issues of proportionality, individual sentencing, and procedural justice. These problems have two interesting comparative settings involving India and the United States, despite the cultural, political, and legal differences between them, as in both legal systems, the death penalty exists and they face similar discussions on wrongful conviction, evaluability of evidence, and the constitutional protection (Banner, 2022; Batra, 2019).

Incorporation of technology in criminal justice has changed the scene remarkably as regards to all levels of adjudication of the death penalty. Digital forensics, biometric identification, robust DNA sequencing, the use of electronic chain-of-custody, and AI-aided investigational technology are becoming more likely to influence the establishment and contamination of culpability (Cole and Lynch, 2020). Advocates claim that technology will increase the reliability, minimize human error and boost procedural protection needed in capital cases. Nevertheless, critics warn that technologies and, in particular, algorithmic tools may introduce racial/caste/socio-economic biases into the system and may only serve to reinforce institutional inequalities within sentencing procedures (Angwin et al., 2016; Hao, 2019). In India as in the United States, these tensions play out loudly in situations of compulsory death penalty when the room to conduct individual judge interrogation is already narrowed.

The jurisprudence of India, which is guided by the theory of the rarest of the rare, was made in Bachan Singh v. State of Punjab (1980) indicates a growing judicial unease with compulsory death sentence. The Supreme Court has over and over again invalidated laws requiring a death penalty as arbitrary, disproportional, and unconstitutional by articles 14 and 21 (Batra, 2019). In the United States the constitutional attacks on the mandate of death sentences have also made use of the aid of the Eighth and Fourteenth Amendments, and the court dictum in the case of Woodson v. North Carolina (1976), which reasoned that any obligation of the death penalties is a breach of the developing values of decency (Steiker and Steiker, 2016). Even with these safety nets in place, there have been fears in the wrongful conviction, unreliable evidence, prosecutor misconduct, and the unfair accessibility to forensic technologies, which again, although not exhibited by technological tools, are all anticipated of by them.

It is on this backdrop that the current research study examines how technology interventions are changing legislation and judicial practice of mandatory capital punishment in India and the United States. It examines the potential to meaningfully reduce historical injustices that are linked to the imposition of

mandatory death penalties with emerging technologies or create new vulnerabilities. Placing this discussion in the context of larger debates on human rights, judicial discretion, and digital governance, the study will play a role in a global discussion about the future of capital punishment in technologically evolving systems of justice.

2. OBJECTIVES OF THE STUDY

The current research paper is aimed at investigating how the judicial and legislative reaction to the mandatory capital punishment in India and the United States is being altered by the technological intervention. Since the two jurisdictions are still grappling with the death sentence and at the same time facing constitutional discourses demanding human-right based due process and fairness, the goals are fashioned to embrace the intricate point of convergence between technology, sentencing policies, and human-right principles. The study objectives will be as follows:

• To examine the legislative systems that exist in support of a mandatory death-penalty policy in both India and the United States, and how, in particular, the statutory frameworks adapt to technological advances in developing evidence, investigating, and sentencing (Banner, 2022; Steiker and Steiker, 2016).

• To investigate how the emergent technologies of digital forensics, DNA sequencing, electronic chain-of-custody solutions, and AI-driven risk assessment affect the evidentiary reliability in capital cases. This goal takes into account the possibility of technological improvements to decrease wrongful convictions or the danger of inherent biases in the system (Cole and Lynch, 2020; Angwin et al., 2016).

• To consider the incorporation of technological evidence in considering mandatory death sentences in the Indian and the USA judiciary. This involves the response to the landmark cases like Bachan Singh in india and Woodson v. The case of North Carolina in the United States and the interpretation of the information presented is whether or not the courts consider that technology has simplified or made sentencing discretion more difficult.

• In order to determine whether the deployment of technology in adjudicating the death penalty amounts to the violation of constitutional and human-rights, specifically whether it violates the principles of due process, proportionality, individualized sentencing, and the safeguarding of arbitrariness (Batra, 2019).

• In order to find out what major challenges and risks are geared towards technological interventions, such as the manipulation of digital evidence, lack of access to advanced forensic tools, bias in algorithms, and, indeed, the process of dependence on machine-generated assessment during sentencing.

• To provide a comparative study of India and the United States to find out whether technology is capable of balancing mandatory death-penalty practices in accordance with the international human-rights regulations or whether the latter can mitigate new vulnerabilities in the procedures.

• To recommend policy assumptions to enhance ethical, legal and procedural measures that should be taken to correct the use of technology responsibly within death-penalty systems so that technological advancements do not undermine constitutional safeguards.

3. LITERATURE REVIEW

Relationships Technology The issue between

technology and criminal justice systems, and capital punishment has become a major focus in modern literature especially because jurisdictions continue to struggle to resolve questions of accuracy, bias, and constitutionality in the adjudication of the death penalty. The works of literatures in India, the United States, and international human-rights organizations show that the new technologies are on the one hand seen as the remedial instrument, and on the other hand, they are considered as the source of new issues. This is a review of the scholarly discussions in four themes (1) the development of the mandatory death-penalty jurisprudence; (2) technology revolution in evidence law; (3) algorithmic tool and sentencing fairness; and (4) comparative constitutional reactions to capital punishment.

3.1 The Mandatory Death Penalty Jurisprudence In Development.

The initial research on capital sentencing focused on the moral and constitutional constraints of mandatory death penalties. In the US, historians track the slow transformation of the mandatory nature of capital punishment to the issues of proportionality and personal responsibility (Banner, 2022). According to legal experts, Woodson v. One of such watershed moments was North Carolina (1976): the Supreme Court invalidated mandatory death sentences because they could not comply with the evolving decency norms under the Eighth Amendment (Steiker and Steiker, 2016). The decision brought in individualized sentencing, an aspect that has remained influential in U.S. Capital punishment cases.

A similar, but separate progress can be shown as an evolution of Indian literature. The statement of the Supreme Court in the Rarest of rare doctrine in the Bachan Singh v. State of Punjab (1980) attempted to impose limitations on judicial discretion, but also limited-focused evaluation (Batra, 2019). The proponents state that conscript capital punishment cannot be equally complied with Articles 14 and 21, which presuppose fairness, non-arbitrariness, and due process (Singh, 2021). Already, the jurisprudence of Indian courts issues with the international human-rights standards since a number of laws that impose mandatory death sentences have since been invalidated (Sharma, 2020).

3.2 Technology and Elevated Reliability in the Cases of Capitals.

The world of evidence has been altered due to technological innovations. DNA profiling, digital forensics, biometric authentication, and cyber-forensics have provided necessity in the investigation of a crime. Evidence indicates that in the United States, the DNA exonerations have resulted in reversal of wrongful convictions even in death cases (Garrett, 2011). Forensic science when institutionally applied makes them more accurate but scholars caution that its reliability should not be overestimated (Cole and Lynch, 2020).

There is an additional layer of complexity with the digital evidence. To avoid tampering and other issues and to guarantee admissibility, the emergence of electronic chain-of-custody systems is present (Goodison et al., 2015). Nevertheless, there is still an apprehension of digital manipulation, creation of metadata, and disparity in the forensic capabilities across jurisdictions (Karie & Venter, 2018). Researchers on India point to lapses in the infrastructures related to

the forensic system, irregular quality of digital-evidence labs, and slow processing schedules, potentially having an unfavorable impact on capital cases (Rai, 2020).

3.3 Algorithmic Tools, Risk Assessments, and Sentencing Bias

The application of algorithmic technologies and risk estimates based on AI has become one of the most debatable trends in the criminal justice field. Predictive algorithms, also known as COMPAS in the U.S., seek to measure reoffending probability. Yet, research indicates such tools have the ability to introduce racial and socio-economic dispositions, which unequally targets the underprivileged sections (Angwin et al., 2016). As Kleinberg et al. (2018) warn, no statistically valid algorithm is capable of eradicating systemic bias due to the fact that datasets tend to mirror historical inequalities.

Algorithms intervention in sentencing is new in the Indian context, but there are threats of such risks, as it has been observed in other cases. Algorithms may cause unintended ultraification of caste and class-based inequalities particularly in a system of justice, in which structural inequalities already occur (Chakrabarti, 2022). Devoid of open auditing guidelines and algorithmic responsibility, AI-helped instruments can undermine due procedure instead of improved it.

3.4 Comparative Constitutional Visions.

Comparative scholarship investigates the ways other jurisdictions meet technology and constitutional protections in capital cases. In America, researchers believe that technological applications have to be reviewed in the prism of the Eighth Amendment, where the reliability of death-penalty adjudication has to increase (Steiker and Steiker, 2016). The forensic evidence, expert testimony, and algorithms have been scrutinized by courts more and more under the due-process requirements.

Indian scholarship also shares the rights-based approach but puts the analysis within Articles 14 and 21. Courts have pointed out that implementing a death penalty must have substantive justification and procedural fairness, transparency, and strict scrutiny of the evidence (Batra, 2019). As people are increasingly using digital evidence, researchers indicate that constitutional protections need to be updated to enable them to cater to emerging technological weaknesses (Rai, 2020).

Its comparative analysis points to similar issues that both jurisdictions encounter because of wrongful convictions, unequal access to forensic expertise, and algorithms discrimination but vary in institutional capacity and loss of history (Singh, 2021). It is always hinted in literature that technology may decrease errors made, but will never replace judicial discretion, ethical protections as well as sound appellate review.

4. PRESENTATION OF PROBLEM/STATE OF HYPOTHESIS.

4.1 Problem Statement

The execution of the death penalty is still plagued with the constitutional issues of evidentiary reliability, judicial discretion, constitutional protection, and institutional bias even in the light of the latest technologies in criminal justice systems. These difficulties are exacerbated by the existence of mandatory capital punishment where the judge is not allowed to try to weigh the circumstances to be

reduced. Of all the cases, Mandatory death sentences in both India and the United States have diametrically opposite constitutionally restrictive landmark cases like Bachan Singh v. State of Punjab (1980) and Woodson v. The statutory provisions and legislative proposals of North Carolina (1976) still cause issues regarding proportionality, fairness, and due process (Banner, 2022; Batra, 2019; Steiker and Steiker, 2016).

The overriding issue that arises out of the literature is that technological tools as much as they can increase the accuracy of evidence also cause new weaknesses. DNA profiling, digital forensics and electronic chain-of-custody enhance precision in investigations however they fail to mitigate the risk of wrongful convictions, procedural and practice fallacies (Garrett, 2011; Cole and Lynch, 2020). Popular in U.S. sentencing, algorithmic risk-assessment tools, in their slow Indian policy advancement, have been determined to incorporate racial, caste-based, or socio-economic biases (Angwin et al., 2016; Chakrabarti, 2022). Being compulsory, death-penalty clauses compound these dangers since they limit personalized judicial examination of cases and elevate the effects of technological errors.

Thus, the focal issue this research paper addresses is whether technology can sensibly help to eliminate structural and constitutional shortcomings of mandatory capital punishment or whether it gives the sense of precision and provokes new aspects of arbitrariness and discrimination. It is this question that is crucial to figuring out how India and United States can come to terms with technological innovation and its relationship with human rights obligations and constitutional provisions of proportionality and fairness.

4.2 Hypothesis

Referring to the existing body of literature and the comparative analysis of the documentaries, the study has the following hypothesis:

H1: Technological innovation-i.e., digital forensics, DNA profiling, and algorithmic aid-can improve the quality and transparency of capital sentencing; however, it will not be sufficient to address the constitutional and structural problems of mandatory death-penalty systems in India and the United States.

H2: In the absence of powerful judicial protection, algorithmic accountability measures and legislative changes, the deployment of technology can increase systematic bias and procedural inazequity in death-penalty trials.

H3: Mandatory capital punishment cannot be applied in modern technological conditions due to the infringement on the ability to impose specific sentencing, which has to be done in individualized manner to assess the reliability and shortcoming of technological data.

In the following sections, actinomy will be used to test these hypotheses by conducting a doctrinal analysis, case studies, and reviewing the empirical evidence that has been obtained through research on forensic-science research.

5. RESEARCH METHODOLOGY

The current research paper will use the approach of qualitative, doctrinal and comparative research to analyze the intersection of technological changes with legislative and judicial policies of mandatory capital punishment in the United States and India. As the research questions involve law provisions, judicial

rationale, constitutional provisions, and the insertion of technology into the criminal justice systems, doctrinal analysis is the main methodological component.

5.1 Doctrinal Legal Research

Statutes, constitutional provisions, judicial and policy documents beneficial to the analysis of mandatory death penalties and technology evidence are analysed using doctrinal research. Within the Indian setting, the discussion confines itself to the provisions of the constitution on Articles 14 and 21 and also landMark cases including Bachan Singh v. The case of State of Punjab (1980) and later case rulings enumerating the constitutionality of the mandatory death sentence (Batra, 2019). United States Doctrinal examination in the United States is founded on the Eighth and Fourteenth Amendments and judicial developments that have been generated as a result of Woodson v. North Carolina (1976), Gregg v. Georgia (1976), and subsequent rulings defining the capital decision (Steiker and Steiker, 2016). This method serves to find out how the courts of the two jurisdictions understand fairness, proportionality, and procedural protection in the death-penalty cases.

5.2 Comparative Methodology

A comparative legal approach is adopted in terms of assessing the way of how India and the United States react to the same issues regarding the mandatory capital punishment and the use of technological devices. Comparative analysis will help the research to discover convergences and divergences in constitutional arguments, legislative changes, and judicial orientations on technology and sentencing discretion (Banner, 2022). This approach also contributes to the placement of both jurisdictions in the larger world trends in human-rights that are against mandatory death penalties.

5.3. Analysis of Secondary Sources.

The research is heavily based on secondary data like books, peer-reviewed scholarly articles, government reports, law-commission reports, forensic-science researches, and the research on algorithmic-risk-assessment tools. The analysis of the effect of technology on accuracy and fairness in capital cases should employ empirical research on digital forensics, DNA evidence, and algorithmic bias (Garrett, 2011; Cole and Lynch, 2020; Angwin et al., 2016). The literature on this subject includes works by scholars based in India and the U.S. that promote the analysis of the present technological capabilities, the deficiencies in infrastructure and the problem of governance.

5.4 Theoretical Framework

The study is placed in the context of a rights-based constitutionalism framework, which emphasizes on the principles of fairness, proportionality, due process and human dignity. The theoretical perspectives used will be:

- Indian jurisprudence Constitutional morality (Batra, 2019)
- Eighth amendment doctrine Evolving standards of decency in U.S. Eighth Amendment doctrine (Steiker and Steiker, 2016).
- Technological due process, which looks at consequences of technologies in procedural fairness and bias (Citron, 2008)

These structures are used to understand whether technology reduces or makes the death penalty administration more complex.

5.5 Scope and Limitations

The research is narrowed down to India and the United States since the two jurisdictions practice the death penalty but base their constitutional and technological arguments differently. Although the study uses forensic-science literature, there are no primary field experimentation and technical testing of forensic instruments. Rather, it analyzes the current empirical research and judicial applications of technology. This provides a relevant legal aspect whilst providing recognition to technicality of the forensic methodologies.

The method to use in the hypothesis testing is to take an agnostic position on a research question.

Through: the hypotheses are tested by:

• Legal commentary Considerations of judicial rulings stating that mandatory death sentences are invalid or limited.

• Comparison of the cases on the evaluation of technological evidence by courts.

• Analysis of empirical forensic-science literature of wrongful convictions, vulnerabilities of digital-evidence, and algorithmic bias.

• Determination of compatibility of technology with the constitutional needs of individualized sentencing and due process.

The paper uses triadic analysis of doctrine, comparative, and empirical knowledge to assess the question of whether technology can help to eliminate structural vices in the mandatory death penalty or whether it will contribute to perpetual inequity.

6. TESTING THE HYPOTHESIS

In the proposed study, there were three hypothesis related hypotheses on the use of technology to rectify the constitutional and structural shortcomings of the mandatory capital punishment option in India and the United States. This part works in support or disapproval of these hypotheses of doctrinal tests, analogy, and review of empirical studies regarding forensic technologies and algorithmic instruments.

6.1 Testing Hypothesis 1

H1: Capital sentencing is better served in terms of accuracy and transparency by technological increase, and fluctuations in constitutional inadequacy cannot be remedied by technological increase.

This hypothesis has a very solid ground in both jurisdictions.

Advantages of technology but partial security.

Advice which includes DNA profiling, digital forensics and biometric verification has had a significant effect in enhancing the accuracy of the evidence. In USA, over 20 death-row inmates have been found innocent through post conviction DNA; they prove that death-row inmates can be cleared of faulty conviction by use of forensic equipment (Garrett, 2011). On the same note, the increasing evidentiary reliability has been enhanced by digital tools of chain-of-custody, as well as enhanced forensic protocols (Goodison et al., 2015).

Nonetheless, these reforms fail to resolve the fundamental constitutive weakness of compulsory death-penalty, namely, the lack of sentencing at the person-level. Both Indian and USA courts have repeatedly concluded that mandatory death penalty goes against constitutional protection as it denies the judges the chance to take into account mitigating factors, mental health, age, socio-economic status or nature of involvement in the crime (Batra, 2019; Steiker and Steiker, 2016).

Therefore, the denial of judicial discretion cannot be given back by even perfection forensic accuracy. Technology enhances evidence, however, it does not solve the structural injustice.

Conclusion: Hypothesis 1 is proved.

6.2 Testing Hypothesis 2

H2: In the event of a lack of powerful judicial protection, technological systems and algorithmic tools can enhance biases in capital cases.

There is vast empirical evidence underlying this hypothesis.

Algorithms and structural inequality.

In the U.S., research on algorithms used to assess the risk of recidivism, e.g., COMPAS, shows racial differences in estimating future criminality with criminal history held constant the black morbidity were over-predicted via the algorithm (Angwin et al., 2016). It means that algorithmic tools tend to reproduce old historical imbalances inherent to datasets.

Researchers in India warn that such risks can also occur when algorithms are exposed to caste and class and policing biases (Chakrabarti, 2022). Considering that India is a country with a multi-layered society, algorithmic decision-making may increase discrimination during the sentencing process, particularly in death penalty cases with marginalized groups.

Digital forensics and disproportionate capacity.

The systems of digital-forensic may also bring inequity by themselves when they are underfunded. As an instance, quality issues in the forensic-lab and backlog in India decrease the validity of a digital evidence (Rai, 2020). In the United States, false confessions and lack of proper expert supervision have led to the wrong conviction of people (Cole and Lynch, 2020).

Algorithms do not necessarily result into fewer but more procedural injustices without robust judicial review, algorithmic transparency requirements and lone forensic audits.

Conclusion: Hypothesis 2 is accepted.

6.3 Testing Hypothesis 3

H3: Compulsory capital punishment cannot co-exist with the current technological conditions of today since it inhibits the personalized consideration of sophisticated technological proof.

Compulsory sentencing and complicated forensic examination.

The two jurisdictions acknowledge that cases of capital must be scrutinized more due to irreversible effects. Existing evidence in modern technologies also in the field of DNA sequencing, probabilistic genotyping, and AI-aided analysis demand critical judicial interpretation. The rigidity of laws on mandatory death penalties removes the flexibility necessary to balance technological evidence, situational aspects and the extenuating circumstances.

Woodson v, the U.S. Supreme Court. North Carolina (1976) clearly affirmed that mandatory capital sentencing would have contravened the Eighth Amendment since a greater weight can not be given on the character and the record of the individual offender. Such personalized evaluation is necessary even more with more complex forensic evidence (Steiker and Steiker, 2016).

Likewise, the doctrine of rarest of rare on Indian Supreme Court presupposes a careful consideration of the situations, the moral guilt of the action, and the validity of the evidence, which cannot be performed

when sentencing is mandatory (Batra, 2019).

Technology demands discretion, not rigidity

Modern forensics instruments demand that judges be familiar with error rates and margins of uncertainty, as well as, methodological weakness. The imposition of a compulsory death penalty eliminates the chances of the judge taking into consideration these uncertainties thus increasing the chances of erroneous justice.

Conclusion: The hypothesis 3 is proved right.

The three hypotheses are each upheld by doctrinal argument, comparative constitutional jurisprudence and empirical research on forensic-science and algorithmic-bias. Technology may be able to reinforce the criminal justice process, but it cannot cure the constitutional flaws of the mandatory death-penalty regimes and it might even bring new forms of arbitrariness without strong safeguards.

7. ANALYSIS

The convergence of technology, the Constitution, and the imposition of obligatory capital punishment brings to light both the fact that neither the United States nor India can afford to keep up with compulsory death penalties in a period of more and more convoluted evidentiary and electronic systems. Even though the two jurisdictions are institutionally different, they still face similar issues related to forensic reliability, algorithmic biasness, and the due-processes.

7.1 Constitutional Capabilities of Authoritative Death penalty.

Articles 14 and 21 have been used in India to oppose the mandatory death penalties. The cases like Bachan Singh v. State of Punjab (1980) and Mithu v. According to State of Punjab (1983), the individualized sentencing is important, and mandatory capital punishment is unreasonable and infringing on the right to life (Batra, 2019). The doctrine of the rarest of the rare is a case-law that mandates courts to consider evidence, culpability as well as mitigating factors before death penalty is awarded.

America is moving along the same path. Woodson v., Supreme Court. In North Carolina (1976), mandatory death sentences were ruled unconstitutional due to their contravention of the E 8 th Amendment by its failure to adhere to the emerging standards of decency. Subsequent cases supported the idea that capital sentencing should take into account the background of the offender, his mental condition, and situations (Steiker and Steiker, 2016).

In this way, both jurisdictions oppose strict sentencing systems- an even more important strategy in the case of a complex technological one.

7.2 Technology and Evidentiary Reliability.

The technology has enhanced accuracy of the criminal investigation, yet there is no error eradication. DNA profiling has vindicated death-row prisoners in the United States proving it to be a frail case of previous convictions (Garrett, 2011). CCTV recovery, location data and mobile extraction are new evidence sources provided by digital forensics, but they are still susceptible to contamination, tampering, and lapses during procedures (Goodison et al., 2015).

India is experiencing the following specific challenges in infrastructure: unstable digital-forensic capacity, labs backlog, and limited chain-of-custody protection (Rai, 2020). These limitations are particularly pronounced in a capital case when the evidentiary scrutiny is to be as maximum.

It takes a special judicial interpretation to handle the

complexity of the modern technology, which is the preventive aspect of mandatory sentencing.

The use of algorithmic tools and structural bias: In this case, the organization must specify how data is organized (whether the data set is structured or unstructured), how it is measured and assessed, and how to execute it.<|human|>Algorithms and Structural Bias 7.3: In this instance, the organization should specify how data is organized (data set is/is not structured), how the data is measured and judged, and how to perform it.

Sentencing and policing algorithmic tools, in particular, COMPAS in the United States, have proven racially unequal and obscures the risk-evaluation methods (Angwin et al., 2016). These tools may appear to be black box in nature, and the courts may find it hard to determine accuracy, rates of error, and a hidden bias.

Indian scholarship cautions algorithmic tools are likely to reproduce caste-based, socio-economic, and policing disparities, were they to be embraced (Chakrabarti, 2022). Algorithms are not necessarily reducing discrimination, which is why, without transparency and good supervision, they could increase it.

Since in mandatory sentencing, individualized evaluation is removed, the technological biased courts cannot be meaningfully considered and rectified. This inconsistency underlines the constitutional argument behind uncompulsory death penalties.

7.4 Comparative Implications

Comparative examination indicates obvious convergence:

• The two jurisdictions demand personalized capital punishment.

• The technology elevates the requirement of seeking judicial review, as opposed to automated and strict penalties.

• The more the forensic complexity is the greater the constitutional guarantees.

Both the Indian doctrine of heightened scrutiny and the U.S. doctrine of evolving standards of decency require a flexible treatment to consider evidence, circumstances and overcome circumstances. Cases of the death penalties as a matter of law contradict these constitutional demands.

7.5 Structural and institutional Concerns.

The two jurisdictions are vulnerable systemically despite technological advancement:

• Lab- forensic error- accidents that may include contamination to expert error (Cole and Lynch, 2020).

• Digital-evidence fragility metadata manipulation, hacking, and gaps in the chain of custody (Karie & Venter, 2018)

• Technological inequality a poor defendant has no access to independent forensic experts.

• Automation bias- there is a risk that judges excessively depend on the results of algorithms (Citron, 2008)

These dangers show that technology is not capable of substituting judicial discretion and constitutions, particularly in the very cases that incorporate indefinite penalties.

7.6 Overall Assessment

The technology can only drive and not reduce the constitutional requirement of individualized sentencing. Although forensic and digital tools improve the accuracy of investigations, they bring in new sources of opacities, fallibility, and bias structures.

Obligatory death-penalty systems are incapable of dealing with the complexity, uncertainty and moral imperatives of such technologies.

Hence, it is necessary that India and the United States incorporate technology in the safeguarding laws- not prescriptive sentencing legislations- to ensure that the due process is upheld and wrongful convictions are averted.

8. RECOMMENDATIONS AND CONCLUSION

Technology and capital punishment have been interconnected it was also found out that despite all its revolutionary potential, technology cannot be used to rectify the inherent constitutional flaws inherent in mandatory death-penalty systems. India and the United States have both shifted towards individualized sentencing as mandated by the courts as it is important to be fair, proportional and give due process as per the cases where irreversible punishment is being administered. In India, jurisprudence created as a result of Bachan Singh v. State of Punjab (1980) and Mithu v. State of Punjab (1983), any death penalty that is made compulsory will contravene Article 14 and 21 by removing judiciary discretion (Batra, 2019). The same happened in United States in which the Supreme Court in Woodson v. North Carolina (1976) invalidated the death sentences that were mandatory due to the failure to satisfy the changing concept of decency in the Eighth Amendment (Steiker and Steiker, 2016). As far as technological innovations are introduced into this legal environment, the incongruence of the Constitution is heightened even further.

Despite the advantages of the evolution of DNA profiling, digital forensics, and the chain-of-custody technologies, which impose fewer limitations on the precision of evidence, they still remain susceptible to systemic flaws such as laboratory inaccuracies, time delays, contamination, and manipulation (Garrett, 2011; Rai, 2020). The sentencing and risk assessment algorithmic tools are even more problematic. The studies of such systems as COMPAS have proven that algorithmic models may incorporate racial, caste-related, and socio-economic biases, which yield results that skew against already marginalised groups (Angwin et al., 2016; Chakrabarti, 2022). Those technological distortions demonstrate that the seeming objectivity of digital systems tends to conceal human biases that flow into the data or design. By eliminating judicial discretion, mandatory death-penalty systems make courts ill-equipped to address such complexities, and thus increase the possibility of entirely commit an irreversible error.

It is due to these reasons that the need to streamline the sentencing structures in both jurisdictions to be in line with the constitutional and technological realities exists. The elimination of the mandatory death-penalty clauses also must be made a legislative project of expression in order to maintain the individualized sentence in all the capital cases. It is also crucial to reinforce quality standards of forensic and digital-evidence, especially using accredited research labs, clear digital chain-of-custody frameworks, and external audit tools that could audit a forensic process and identify areas of weakness (Goodison et al., 2015). Algorithms and other technological tools should undergo a transparency, accountability, and judicial review process, whereby the prospective defendants have chances to actually question both the processes and assumptions behind digital evidence.

There is need to train judges, prosecutors and defence lawyers to improve the skills they have on forensic and technological techniques to allow them not to misinterpret or over rely on complex scientific evidence in capital cases (Citron, 2008). Independent forensic experts should also be availed to indigent defendants to ensure that no person is sentenced to the death penalty without equal opportunity to challenge technological evidence. Lastly, appellate courts need to embrace a more demanding and technologically aware paradigm of adjudicating the death-penalty go-round, which integrates both law with science-literacy and avert false-carryments of justice. In the United States and India, it is possible to make capital sentencing systems more human-rights friendly so that the promotion of sciences and technologies are not excessively overvalued to the constitutional rights to the dignity and life of the accused.

Reference

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: There's software used across the country to predict future criminals. And it's biased against Blacks. ProPublica. https://www.propublica.org/article /machine-bias-risk-assessments-in-criminal-sentencing

Banner, S. (2022). The death penalty: An American history (Updated ed.). Harvard University Press.

Batra, N. (2019). Constitutional morality and the death penalty in India. NUJS Law Review, 12(3), 421–450.

Chakrabarti, A. (2022). AI, caste, and criminal justice in India. Indian Journal of Law and Technology, 18(1), 45–67.

Citron, D. K. (2008). Technological due process. Washington University Law Review, 85(6), 1249–1313.

Cole, S., & Lynch, M. (2020). The social and cultural impacts of forensic technologies. Annual Review of Law and Social Science, 16, 145–164.

Garrett, B. L. (2011). Convicting the innocent: Where criminal prosecutions go wrong. Harvard University Press.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system. RAND Corporation. https://www.rand.org/pubs/research_reports/RR879.html

Karie, N., & Venter, H. S. (2018). A formal digital forensic investigation framework. Forensic Science International: Digital Investigation, 26, 90–102.

Kleinberg, J., Lakkaraju, H., Leskovec, J., Ludwig, J., & Mullainathan, S. (2018). Human decisions and machine predictions. Quarterly Journal of Economics, 133(1), 237–293.

Rai, S. (2020). Digital forensics and fair trial rights in India. Indian Law Review, 4(2), 150–175.

Sharma, R. (2020). Mandatory death penalty and Indian constitutional law. Journal of Indian Legal Studies, 6(2), 112–134.

Singh, M. (2021). Due process, proportionality, and the death penalty in India. National Law School Journal, 32(1), 77–100.

Steiker, C. S., & Steiker, J. M. (2016). Courting death: The Supreme Court and capital punishment. Harvard University Press.

REGULATING ONLINE PLATFORMS: THE EFFECT OF ONLINE HARRASMENT AND HATE SPEECH ON WOMEN'S ENGAGEMENT IN POLITICAL ACTIVITIES

Alexander C[1]

Dr. B. Venugopal[2]

ABSTRACT

The internet was once viewed as a space of equality, a democratic platform where every voice could be heard without barriers. Yet for women entering political conversations online, this vision often collapses under the weight of harassment, hate speech, and targeted abuse. This paper examines how these forms of digital hostility impact women's political participation, both by silencing their voices and by shaping the culture of fear that surrounds female presence in public discourse. Online trolling, defamation, and threats of sexual violence have become powerful tools that discourage women from speaking out, influencing debates, or taking on leadership roles. What begins as a conversation quickly becomes a confrontation, forcing many to withdraw or self-censor to survive in spaces that should have empowered them.

Through case analyses and a review of current regulatory frameworks, the study highlights the disconnect between the protection promised by law and the reality women face in digital spaces. Despite platform guidelines and cybercrime legislation, responses remain inconsistent, delayed, and largely indifferent to the gendered nature of online abuse. The failure to recognize this difference reinforces a culture where women's voices are undermined, and democracy loses its inclusivity. This paper argues that the regulation of online platforms must move beyond technical enforcement and address the deeper social and cultural biases that drive gender-based digital violence. True reform demands accountability from platforms, empathetic lawmaking, and a collective effort to create safer online environments. Only when women can speak without fear, lead without restraint, and engage without hostility will digital participation fulfil its democratic promise. Until then, the internet remains an unfinished revolution — powerful, yet profoundly unequal.

I. INTRODUCTION

People used to think of the digital world as a new kind of public space where anyone can freely share ideas without the barriers of the class, gender, and geography. The internet assured to make information and power more equal, to break down hierarchies, and to start conversations. That vision seems far away now particularly for women who want to talk about politics online. This online platform should be a place of freedom but it has become a place where targeted aggression and outright hatred of women can grow.

Digital platforms seemed to express yourself and get involved in your community in olden days. But in today's world, online harassment, hate speech, and sexualized insults are just common. In this paper the impact of online harassment on women's political participation will be examined. Gendered abuse not only hurt people but it also makes women quiet and

[1]*Research Scholar, School of Law, Vel Tech Rangarajan Dr. Sagunthala Rangarajan Institute of Science and Technology, Avadi, Chennai*

[2]*Professor and Dean, School of Law, Vel Tech Rangarajan Dr. Sagunthala Rangarajan Institute of Science and Technology, Avadi, Chennai*

forces them out of online spaces, it changes the environment of political debate. Defamation, trolling and sexual threats are the new ways to keep women out and make democratic conversation a war zone in online platform.

If we look around the world, all the current laws and policies to show how both the law and technology have not been able to stop gender-based violence in the digital space. There are

laws against cybercrime but they aren't always enforced properly, and when they are enforced, they will not always consider women's real experiences. To stop online harassment, it requires more than just deleting abusive posts or banning trolls. This implies changing our laws, institutions, and attitudes, as well as the way we live is required.

To make real change happens digital platform needs to fulfil their duties. Policymakers need to prioritize gender at the center of their responses. It is essential for the society to realize that online safety is important for women to engage fully in democracy. The internet will only reflect the same old inequalities until women can speak out, take on leadership role, and participates in digital debates without fear.

Literature Review:

Women, Politics, and the Digital Realm:

Over the past decade, researchers and advocacy groups have focused on how gender affects how people participate in politics and talk about politics online. There is a lot of proof that women use the internet differently than men, especially when they are in public or political roles. (Osei-Appiah et al., 2023)

The Gendered Aspect of Digital Harassment:

Women who work in politics, journalism, or activism get a lot more hate online than men do. A meta-analysis of 48 studies found that more than 80% of women said that online harassment made them feel bad. More than 60% changed how they acted online to get away from abuse. What worries me the most? Because of the pressure, about one in five women stopped going to public events or left political platforms altogether.

It's not just how often women are attacked that stands out, but also how the attacks happen. People might criticize men for what they think, but women are much more likely to be attacked for who they are, how they look, their gender, or their identity. It's not just what they say that hurts; it's also that they're trying to push them out. (FAQs: Digital Abuse, Trolling, Stalking, and Other Forms of Technology-facilitated Violence Against Women and Girls | UN Women – Headquarters, 2025)

Worldwide Trends and Local Differences:

Online violence against women is everywhere around the world. Surveys show that about 60% of women who are Members of Parliament in the Asia-Pacific region have been the victims of online gender-based violence including sexual threats, character assassination, and cyberstalking, furthermore Women in politics in Latin America, especially those who are Indigenous, Afro-descendant, or LGBTQ+ encounter even more severe instances of digital hate. (Tavares & Wodon, 2018)

The scenario in Europe is pretty similar. Research from Sweden reveals that women in politics get more personal and sexualized attacks than men do. These attacks make fun of their skills, their character. A lot of women end up silencing themselves holding back or even stepping away from the discussion, but their male colleagues keep talking without hesitation.

Effect on Political Participation:

Online harassment isn't just a personal problem, it impacts democracy as a whole. Digital spaces are now where most political discussions, campaigns, and decisions take place. The whole system crumbles when women face harassment and are silenced. Morini, 2025 says that toxic online spaces make women refuse to run for office, step down from leadership, or keep quiet instead of speaking up. What happened? Less variety in public policy and a political culture that stays stuck in old, male dominated ways.

Cultural and Structural Dimensions:

There is no such phenomenon as unintentional online gendered violence. Digital platforms are designed in such a way that they reward anger, drama, and anything that goes viral. This creates a perfect environment where harassment booms. Social media gives criminals anonymity and a large audience, which makes them more daring and less responsible. At the same time, old fashioned sexist attitudes are just as common online as they are in real life, which keeps the same power structures in place. Experts argue that online abuse is not merely random cruelty, it represents a modern method of enforcing gender norms, penalizing women who resist patriarchal dictates. (Sinha et al., 2017)

This research keeps coming back from four main ideas:

Gendered asymmetry:

Women face unique sexualized attacks that are based on their identity.

Emotional and professional consequences:

Harassment negatively impacts women makes them to feel bad and stops them from secure position in politics or the public sector.

Institutional failure:

Legislation, technology firms, and law enforcement agency are insufficient to protect victims.

Democratic erosion:

Suppressing women online makes democracy less legitimate by taking away their voices.

The internet doesn't create equality for all. It highlights and even makes worse the unfairness present in the physical world. When women are pushed out of digital political spaces, it hurts more than just women; it hurts democracy as a whole.

How Online Harassment Makes Women Quiet:

Online harassment does not just occur to women, it works as a structure to keep them quiet and push them out. If you look at any social media feed or forum, you will see the same thing occur, women are abused all the time. Some attacks are highly personal in nature, while others are strategically planned and made public. These are not random, sexualized insults, dogpiling, and planned smear campaigns. They want women to feel small, scared, and unsure if it is not worth it to speak up. There are more than just emotional effects, though. Women are excluded from discussions that influence our digital world, careers stall, and chances disappear. The message is clear, remain silent or face the consequences.

Fear and Mental Damage:

When someone stalks you online, fear takes over quickly. Women who express their opinions in public or political arenas are mocked, humiliated, and attacked personally over and over again. People restrain themselves because they are aware that any post, comment, or photo can trigger a wave of

harassment. The internet, which should be a place where people can talk to each other freely, is starting to feel like a minefield. People don't share their views as freely anymore. They become more cautious and carefully consider their words and even worry about what comes next.

Harassment can take many forms, such as:

Trolling is when groups intentionally insult or provoke people to stop them from expressing their opinions.

Doxing is when personal information like phone numbers or addresses is made public, which can put people in danger in real life.

Sexual threats and cyberstalking like sending around altered or private pictures.

Censorship of oneself:

Self-censorship is not just avoiding things, it is a way for women to protect themselves from harassment. It is not about disappearing completely. Instead, they might post less, stay away from controversial topics, or change what they say so it won't get them in trouble. A shocking finding from the 2020 global study by Amnesty International found reveal that 39% of women stopped using social media after experiencing harassment and 29% left the social media platforms entirely. Women still scroll and watch, but they stopped voicing their opinions. It is like they are quietly backing off. They fade into the background, present but quiet, and are no longer part of the conversation.

Discouraging Leadership:

Women in leadership roles including politicians, journalists, and activists frequently face harassment. These attacks are unrelated to their ideas or policies. They target on character, intelligence, and emotional stability, using personal identity as a weapon. This is not just a coincidence. It is a planned effort to undermine authority and trust and keep women from making decisions. Every insult or smear isn't random, it serves to maintain outdated patriarchal norms in place and scare off anyone who might want to follow in their footsteps.

Taking away legitimacy

Women who are still visible face yet another struggle. Harassers use fake news, gendered stereotypes, and fake pictures to make people doubt their skills and honesty. Lies and fabricated scandals don't go away, they stay online and change how people see things for years. It's clear from research in media psychology that the more sexist content people see, the more likely they are to think that women shouldn't be leaders. Digital spaces become battlegrounds where women's rights are questioned, doubted, and attacked over and over again.

Consequences for the system:

Women encounter fear, self-censorship, and damage to their reputations, and these things are not merely negative consequences. They indicate that online harassment is planned to maintain gender hierarchies. Digital violence does not just replicate power imbalances that happen in physical world, it changes them for the digital era. This is not just a rude behavior. It is a system that prevents women from attaining power and keeps men dominant in public life.

Why Current Systems Aren't Working:

Cyber laws and corporate policy claims to protect users, however women are still at risk in the online platform. Systemic failures go deep, and they have to do with how laws are crafted, how institutions work, and what tech companies prioritize. Finally, people are

recognizing that online harassment is a real problem. But when it comes to accountability? What about enforcement? Still slow, broken, and way too often blind to the impact of online abuse on women.

1. Policies that don't take gender into account

A fundamental issue is that many laws and platform regulations claim to be neutral. They act like harassment affects everyone equally, even though women are more prone to face sexualized, identity-based, and deeply psychological forms of abuse. Women are the main targets of offences such as sharing images without permission, revenge porn, and deepfake pornography. But the law doesn't constantly recognize these as crimes against women. When policies overlook the gendered roots of abuse, they make it seem normal, turning a structural problem into a supposedly neutral one and making women's experiences invisible in the eyes of the law.

2. Weak enforcement

Even when there are laws, they are not always followed. Bureaucracy often leads to reports being misplaced or discarded. Instead of receiving assistance, victims face doubt and blame. Many police departments lack the necessary training or the awareness of gender issues that they need to look into cybercrimes. Instead of going after the people who did the crime, the police ask victims about their online activities, which makes people less likely to believe them. People who do bad things learn that they can do them with little risk. For a lot of women, the pursuit of justice ends up hurting more than the harassment itself, keeping them stuck in cycles of silence and giving up.

3. No Interest in Platforms

Facebook, Instagram, X, and other tech companies own the online spaces, yet they fail to address harassment with the seriousness it deserves. There are reporting mechanisms and guidelines, but they are usually just for show and meant to protect the platform's image more than the safety of its users. Algorithms miss abuse content that is hidden behind jokes and sometimes flag the wrong posts. Relying solely on Automated moderation isn't enough for real accountability. It needs transparency trauma-informed reporting, human moderators who are trained to be aware of gender related issues, and a genuine commitment to changing the way people act online. Most platforms are far from achieving this.

4. Problems with Global Jurisdiction

The internet does not care about borders and that makes it very hard to enforce rules. Harassment knows no borders, a offender in one country can target a victim in another using servers located all over the world. The legal system has struggled to adapt. Authorities find it challenging to figure out who has the right to act, how to gather evidence, or even how to impose penalties on people across borders.

Most legal systems operate within their own borders, but tech companies do business all over the world. Because there is not much international collaboration, criminals can evade justice through the cracks, find loopholes, and leave victims vulnerable. The potential gain remains substantial, but the risk for the people who do it is still low. Online harassment is still a crime that is easy to commit and hard to punish without international accords and cross-border collaboration.

Consequences for the system:

When you add up gender neutral laws, weak implementation, platform indifference, and these gaps

in jurisdiction, you get a perfect storm. Online harassment not only persists, but it also escalates. Most of the time, the people who is responsible for these things get away with it, and women pay the price in terms of their mental health, social lives, and careers. We must view these failures as part of a bigger problem, not just a few mistakes. That's the only way to make interventions that work and to get people to trust digital environments.

Effect on Democracy

Harassment online is not just a personal issue, it threatens the very idea of democracy. When online spaces become aggressive, particularly towards women, they cease to function as venues for open discourse and public participation. For democracy to work, everyone needs to be able to speak up. Silencing women online not only harms them, but it also hurts representation and the whole legitimacy of the system.

1. Less Public Debate

A healthy democracy needs a lot of different kinds of voices. Harassment based on gender makes that range smaller by keeping women out of public discussions. Many women stop or hesitate to share their views after being made fun of, threatened, or humiliated enough. That takes away different points of view from public discussion.

Digital platforms were meant to let everyone in, but now they mostly just repeat the loudest, most aggressive voices, which are usually men. Harassment is like a gatekeeper that decides who can join the conversation and makes real equality depend on how well someone can handle abuse.

2. Loss of Future Leaders

Harassment does not only hurt today's voices it also makes tomorrow's leaders less likely to speak up. Young women observe politicians, journalists, and activists getting harassed all the time, and they quickly learn that being in the public eye has its costs. This feeling of danger kills ambition and makes many people censor themselves before they even enter public life.

When women are not in the leadership position, the government does not listen to half of the people and does not make decisions that are good for everyone. The cycle keeps going fewer role models, fewer representation, and men remaining in power.

3. The decline of equality in digital spaces

People thought the internet would make things fairer, where ideas were more important than gender or class. Things are different in real life. Online spaces often make offline inequalities worse. When women are pushed to the edges, equality stays an idea and not a fact.

4. Less trust and civic involvement

People lose faith in not only platforms, but also institutions and democracy itself when online abuse is allowed to run wild. People think that governments and businesses are either powerless or do not care about keeping things fair when harassment is not stopped. People are becoming more cynical and are withdrawing from civic life.

That lack of interest does not stay online. It sneaks into activism, public debate, and politics in the real world. In the end, online harassment hurts democracy because it makes people question whether their voices matter.

5. The rise of misinformation and polarization

Harassment based on gender makes people more divided and spreads false information. Algorithms on

social media sites like Facebook and Twitter reward anger, not reasoned debate. When women are silenced, discussions become more combative, less reasoned, and more broken up. This is because women often bring collaborative and empathetic points of view.

Harassment makes people more divided and comes from it, making things worse for civic culture. It makes it harder for us to make smart choices and keeps democracy from being stable.

The Way Forward: Making Digital Spaces Safer

We need more than quick fixes or changes to algorithms to stop online harassment of women. The problem is deep seated, stemming from power imbalances and ingrained in the very structure of the internet. For real change to happen, there needs to be a coordinated effort on many fronts, such as the law, technology, institutions, and culture.

1. Making Platforms Responsible

Social media companies control what we do, say, and see online. But too often, they have not taken real responsibility for harassment on their sites. Their rules change all the time, their moderation is not always good, and when it comes down to it, they still put safety behind profits and user engagement.

That needs to change. Platforms should make public, clear reports about how many harassment cases they get. How fast do they get back to you? Do they really punish people who break the law more than once? If they really care, they will make their reporting systems easy to use, available in many languages, and aware of how traumatic it is for victims. Survivors need to be able to write down what happened, keep track of their cases, and get updates without getting lost in a maze of forms.

It's not enough to just use AI to fix this. Algorithms do not take into account the context, miss small threats, and sometimes silence the wrong people. Companies need to hire and train human moderators who know the ins and outs of digital ethics and gendered abuse.

But technology fixes alone won't change the way people use the internet. Platforms should take the lead and show the way. Work with groups that support women's rights, researchers, and lawmakers. Not just empty slogans, but real campaigns that promote respect, inclusion, and empathy.

2. Laws and policies that take gender into account

Laws are important. Most current rules treat all online abuse the same, but that does not take into account the unique harms that women face. Governments need to make it clear that things like non-consensual image sharing, deepfake porn, cyberstalking, and sexual extortion are all illegal.

It's not just about making new laws. Judges and police need to know how these crimes work. That means learning how to do digital investigations, how to be sensitive to gender, and how to deal with trauma. Fasttrack complaint systems, legal aid, and access to mental health care can all make a big difference. People who have survived need to know that the system is on their side, not against them.

Laws by themselves don't change people's minds. Legal changes should go along with public campaigns and education that focus on digital ethics, gender equality, and how to behave respectfully online. It is time to treat women's safety online as a basic right.

3. Changes in culture and education

You cannot make a culture problem go away with laws. Old patriarchal ideas are what lead to online abuse, and

it will take a whole generation to get rid of them.

Begin in the classroom. Kids should learn how to be good digital citizens, how to act morally, how to spot false information, and how to stand up to bullying. Teach people to care about others. Teach people how to read the news. The goal is to raise a new generation of digital citizens who will speak out against abuse.

Politics, journalism, activism, mentorship, and safe networks are important to women in public life. It's easier to speak up and keep going when there are programs that connect women, give them advice, and help them feel like they are part of a group. Take Back the Tech and other grassroots campaigns or Reclaim the Internet show how people can work together to take back online space and make it stronger.

It takes time to change culture. Jokes, the news, and everyday language all play a part. Teachers, influencers, and the media can push new stories that show that digital abuse is not just a "women's problem," but a failure of society as a whole.

Making digital spaces safer isn't a one-time thing. It is an ongoing promise to rethink laws, redesign platforms, and question the old stories we tell about who belongs online.

Conclusion:

People say a lot of good things about the internet. They say it is one of the greatest things we have ever done, a tool that connects people all over the world, spreads information, and gives us power. But for a lot of women, this promise doesn't mean much. The digital world often just repeats the same old problems that women face in real life, instead of giving them real chances or safety. What began as an aspiration for transparent, democratic discourse has, in numerous instances, devolved into yet another domain of exclusion, where gender based harassment marginalizes women from public discourse and civic engagement.

I have demonstrated in this paper that online harassment is not merely the behavior of a few malicious individuals. It is a part of the system. It decides who can really take part in democracy. Women on digital platforms face targeted abuse and attacks meant to scare them, ruin their reputations, and scare anyone who tries to speak out or lead. These are not just personal wounds; they silence voices, keep women from becoming leaders, and make people less likely to trust the government. That leaves a democracy running on empty. When women step back, everyone loses. We lose new ideas, we lose the ability to care about others when making decisions, and we lose any chance of real fairness.

Why does this keep happening? It all comes down to deep, structural problems. Most laws and platform rules don't care about gender at all. They act like abuse is a neutral issue that doesn't affect women more than men. When there are rules, they are rarely followed. This is because authorities don't have enough training, procedures take too long, and survivor centered approaches are not common. The internet is global, which makes things even harder. Crimes that happen across borders can go unnoticed. These gaps add up, keeping women from speaking out and letting abusers get away with it.

So, what should we do? We need to work together on three levels. First, tech companies need to be more open, design with everyone in mind, and have real people in charge of oversight. Second, governments

must be passed laws that recognize gender, teach police and courts how to respond correctly, and speed up the process of getting justice, with survivors at the center.

Third, societies need to change the culture from the ground up, with education, mentoring, and public campaigns that make empathy and equality the norm, not the exception.

For any real democracy, a safe internet is not something extra or special; it is necessary. You can tell how healthy a democracy is by whose voices it lets in and whose it shuts out. The internet can still connect people and change their lives, but it can only do that if women are not only there, but also heard and respected. The digital age's promise is still not fully realized. It was supposed to bring equality, but it still sounds like inequality. When the online world stops using old hierarchies and makes room for an equal future, real progress happens.

References:

1.Osei-Appiah, S., Mutsvairo, B., & Orgeret, K. S. (2023). Women and digital political communication in non-Western societies. Information Communication & Society, 26(13), 2507–2517. https://doi.org/10.1080/1369118x.2023.2257995

2. FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women and girls | UN Women – Headquarters. (2025, February 10). UN Women – Headquarters. https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women

3.Tavares, P., & Wodon, Q. (2018). ENDING VIOLENCE AGAINST WOMEN AND GIRLS: GLOBAL AND REGIONAL TRENDS IN WOMEN'S LEGAL PROTECTION AGAINST DOMESTIC VIOLENCE AND SEXUAL HARASSMENT.

4.Morini, C. (2025, June 13). Countering online sexist hate speech in the European legal context: Between present commitment and future challenges - QIL QDI. QIL QDI. https://www.qil-qdi.org/countering-online-sexist-hate-speech-in-the-european-legal-context-between-present-commitment-and-future-challenges/#:~:text=%5B1%5D%20UN%20HRC%2C%20'Accelerating%20efforts%20to%20eliminate,July%202018)%20UN%20Doc%20A/HRC/RES/38/5%20para%202.

5. Sinha, P., Gupta, U., Singh, J., & Srivastava, A. (2017). Structural violence on women: An impediment to women empowerment. Indian Journal of Community Medicine, 42(3), 134. https://doi.org/10.4103/ijcm.ijcm_276_15

HOW AI TOOLS CHALLENGE TRADITIONAL METHODS OF LEGAL INTERPRETATION: A COMPARATIVE ANALYSIS WITH INDIAN CONTEXT

Dr. Pranav Ranga[1]

Mr. Rahul Mehra[2]
Research Scholar

ABSTRACT

The rapid emergence of Artificial Intelligence (AI) tools in the legal sector has significantly transformed traditional legal interpretation across global jurisdictions. In India, where legal interpretation is deeply rooted in constitutional morality, purposive construction, precedent-based reasoning, and socio-legal context, the integration of AI presents both opportunities and challenges. This paper examines how AI-driven legal tools interact with, support, and sometimes disrupt conventional interpretive functions in India. Through comparative analysis with the United States and European Union, it evaluates the capacity of AI to replicate or supplement human judicial reasoning while addressing concerns of opacity, bias, democratic legitimacy, and accountability. The study proposes a hybrid human-AI interpretive model and recommends regulatory, ethical, and pedagogical strategies for responsible integration of AI in legal interpretation.

Keywords: *Artificial Intelligence, Legal Interpretation, Algorithmic Decision-Making, Comparative Law, Legal Reasoning*

I. INTRODUCTION

Legal interpretation forms the backbone of judicial functioning. It determines how statutes are read, how constitutional provisions evolve, and how judgments contribute to the development of legal principles. Traditionally, Indian courts have adopted interpretive approaches that are human-centered, value-driven, and deeply contextual. Cases such as Navtej Singh Johar v. Union of India and KS Puttaswamy v. Union of India reflect the judiciary's reliance on moral reasoning, empathy, social realities, and constitutional vision.

The integration of Artificial Intelligence (AI) into this interpretive environment marks a significant shift. AI tools promise efficiency, rapid data retrieval, automated analysis, and predictive insights. Yet, they also raise fundamental questions: Can AI truly interpret law? Does AI-generated reasoning align with constitutional values? What are the implications for judicial accountability and democratic legitimacy?

This research paper explores these questions comprehensively, focusing on India while drawing comparative observations from the United States and European Union, where AI tools such as predictive judicial algorithms, research aides, and AI-based legal analytics have been operational for longer periods.

2. OBJECTIVES OF THE STUDY

The principal objectives of this research are:

1. To examine how AI tools are being integrated into the Indian judicial and legal interpretive system.

2. To identify the challenges AI poses to traditional judicial and legal interpretive methods in India.

3. To conduct a comparative analysis of AI-based legal

[1]*Assistant Professor, M.M. (Deemed to be University), Mullana, Ambala*

[2]*M.M. (Deemed to be University), Mullana, Ambala*

interpretation models in India, the United States, and the European Union.

4. To analyze whether AI-driven interpretation aligns with the constitutional ethos and jurisprudential foundations of India.

5. To evaluate existing regulatory models addressing AI in law, particularly the EU AI Act, and their relevance to India.

6. To propose a hybrid, human-centered model that incorporates AI responsibly while ensuring judicial autonomy and constitutional morality.

3. LITERATURE REVIEW

3.1 Traditional Legal Interpretation in India

Indian legal interpretation relies heavily on constitutional morality, purposive reading, and evolving social values. Scholars such as Upendra Baxi, Sujit Choudhry, and Aharon Barak emphasize that interpretation is not merely mechanical rule application; it is a moral enterprise that requires understanding context, culture, and human consequences.

Indian courts employ various interpretive methods:

- **Literal interpretation** (plain meaning rule)
- **Purposive interpretation**
- **Harmonious construction**
- **Constitutional morality**
- **Doctrine of contemporary needs**

Research shows that these methods rely on human intuition, ethical judgment, societal awareness, and judicial discretion—all aspects difficult to encode into algorithms.

3.2 Rise of AI in Legal Systems

Global literature highlights the increasing use of AI tools like:

- Machine learning-based prediction systems (e.g., COMPAS in the U.S.)
- AI legal research tools (ROSS Intelligence)
- AI-enabled translation and summarization (e.g., SUVAAS in India)
- Algorithmic sentencing aids
- Contract review automation tools

Scholars such as Lawrence Lessig and Frank Pasquale warn that algorithmic decision-making may embed opacity ("black-box algorithms") and reproduce biases present in historical datasets.

3.3 AI and Judicial Decision-Making

Studies show that AI systems excel in tasks involving:

- Data sorting
- Pattern recognition
- Precedent retrieval
- Classification

However, they struggle with:

- Normative interpretation
- Moral reasoning
- Cultural sensitivity
- Constitutional balancing tests
- Judgment writing based on equity

Legal scholars emphasize that judicial interpretation requires empathy, understanding of socio-political context, and the ability to evaluate human consequences—dimensions not replicable by most current AI systems.

3.4 USA and EU: Global Perspectives

In the United States, AI tools like COMPAS have been criticized for racial bias in sentencing predictions. In State v. Loomis, the court expressed concerns about lack of explainability. The EU AI Act classifies legal-sector AI systems as "high risk," requiring

transparency, human oversight, and accountability. Comparison with India highlights the urgent need for structured regulations and ethical frameworks.

4. PROBLEM STATEMENT AND HYPOTHESIS

Problem Statement

AI-driven tools pose fundamental challenges to traditional legal interpretation in India by potentially undermining judicial discretion, constitutional morality, and human-centered interpretive methods. Yet, they also offer opportunities for enhancing efficiency and access to justice. The core problem lies in determining the extent to which AI can assist without replacing human judicial reasoning.

Hypothesis

H1: AI tools challenge traditional methods of legal interpretation by introducing opacity, bias, and potential displacement of judicial discretion.

H2: A hybrid human-AI model can strengthen interpretive integrity, provided AI is used only as an assistive tool under strict regulatory and ethical controls.

5. RESEARCH METHODOLOGY

This study adopts a qualitative doctrinal research methodology supported by:

1. Doctrinal analysis of statutes, judicial decisions, AI-based legal tools, and technological frameworks.
2. Comparative method examining approaches in India, the U.S., and the EU.
3. Case-law examination, including Indian landmark judgments.
4. Policy analysis, including the EU AI Act and U.S. algorithmic accountability debates.
5. Secondary sources, such as academic journals, reports, and scholarly commentaries.

This methodology enables a theoretical and critical examination of the interplay between AI and traditional legal interpretation.

6. ANALYSIS AND DISCUSSION

6.1 Why AI Cannot Fully Replicate Human Legal Interpretation

6.1.1 Contextual and Moral Reasoning

Indian courts often rely on moral reasoning and constitutional ethos rather than strict textualism. For example:

- *Navtej Singh Johar:* legality shaped by dignity, equality, privacy
- *Puttaswamy:* recognition of privacy as a fundamental right

AI lacks moral imagination and cannot interpret concepts such as *constitutional morality, equality of status, or transformative justice.*

6.1.2 Socio-Legal Sensitivity

Legal interpretation involves understanding:

- Caste dynamics
- Gender issues
- Socio-economic realities
- Historical discrimination

AI systems trained on past judgments may reproduce embedded discriminatory patterns.

6.1.3 Reasoned Judgments vs. Algorithmic Output

Indian law mandates reasoned judgments (as in Ajay Hasia). Algorithms, especially deep neural networks, provide outputs without transparent reasoning, violating judicial standards.

6.2 Benefits of AI in Legal Interpretation

Despite challenges, AI offers significant benefits:

- Speed in searching precedents and relevant statutes.
- Automated translation (e.g., SUVAAS).

• Pattern detection in case-law trends.

• Predictive analytics to assist lawyers.

• Reduction in case pendency through automated administrative assistance.

Hence, AI should be viewed as a supplement, not a replacement.

6.3 Comparative Analysis: India, USA, EU

India

• AI tools are assistive (SUPACE, SUVAAS).

• No comprehensive AI regulation.

• Judicial reliance on constitutional morality restricts automation of judgment.

USA

• Advanced predictive tools (COMPAS, ROSS).

• Issues: bias, racial discrimination, lack of transparency.

• Courts increasingly skeptical of automated sentencing.

EU

• EU AI Act imposes strict regulatory requirements.

• Legal AI classified as high risk due to potential societal harm.

• Emphasis on explainability, human oversight, accountability.

India stands to benefit from adopting similar safeguards.

7. TESTING THE HYPOTHESIS

Hypothesis 1: AI challenges traditional legal interpretation

Supported by:

- Evidence of algorithmic bias (U.S. case studies).
- Black-box nature of AI inconsistent with Indian judicial requirements.
- Risk of undermining judicial independence if AI influences interpretation.

Result: Hypothesis 1 is supported.

Hypothesis 2: A hybrid human-AI model can protect interpretive integrity

Supported by:

- AI's usefulness in legal research, translation, and document review.
- Judicial need for human moral reasoning and discretion.
- Comparative models (EU) demonstrating safe use through human oversight.

Result: Hypothesis 2 is strongly supported.

8. CONCLUSIONS

The integration of AI in legal interpretation presents a complex interplay of opportunities and challenges. While AI enhances efficiency, speed, and data analysis, it lacks the moral, contextual, and empathetic qualities required for genuine legal interpretation—especially in a constitutional democracy like India. AI tools risk reproducing historical biases, undermining judicial discretion, and compromising transparency unless carefully regulated.

A cautious, human-centered approach is necessary. The judiciary must retain ultimate interpretive authority, and AI must remain a supportive instrument. The comparative analysis highlights that India must develop strong regulatory frameworks similar to the EU and avoid pitfalls observed in the U.S. system.

9. Recommendations

1. Adopt a Hybrid Interpretive Framework

AI should support, not replace, judges and legal scholars.

2. Develop a Comprehensive AI-in-Law Regulatory

Act

India should adopt a regulatory framework inspired by the EU AI Act, mandating:

- Explainability
- Human oversight
- Transparency
- Accountability

3. Mandatory AI Impact Assessments for Judicial Tools

Before deployment, tools like SUPACE require testing for:

- Bias
- Reliability
- Data quality

4. Judicial Training in AI Literacy

Judges and lawyers must be trained in understanding AI outputs and limitations.

5. Ethical Standards for AI Developers

Private developers of legal AI tools must adhere to ethical guidelines ensuring public accountability.

6. Strengthen Data Governance

Ensure high-quality, bias-free, and representative datasets.

7. Promote Interdisciplinary Research

Encourage collaboration between legal scholars, technologists, and ethicists.

RE-IMAGINING COPYRIGHT GOVERNANCE IN INDIA: LEGAL AND ETHICAL CHALLENGES IN THE AGE OF ARTIFICIAL INTELLIGENCE

Maitri Shail Patel[1]
Dr. Sonal Raval[2]

ABSTRACT

The rapid integration of Artificial Intelligence (AI) into creative, cultural, and commercial ecosystems has fundamentally transformed the contours of authorship, originality, and ownership — the very pillars of copyright law. The rise of AI-generated works presents previously unheard-of ethical and legal challenges in India, where copyright jurisprudence is primarily based on the human-centric model of the Copyright Act, 1957.

This research paper critically examines the challenges of aligning existing copyright frameworks with the realities of algorithmic creativity and machine-generated outputs. It investigates whether authorship, liability, and fair use issues in the era of intelligent automation are sufficiently addressed by the current legislative provisions, case law interpretations, and international commitments under TRIPS and the Berne Convention.

The study also looks into the ethical implications of AI in creative processes, including the rights of human creators whose work is used to train generative models, biases present in training datasets, and transparency in authorship attribution. In order to suggest a fair, forward-thinking governance model for India, it also assesses comparative legal developments across jurisdictions, such as the US, UK, and EU.

The study emphasizes the need for a nuanced approach that balances innovation and protection, human creativity and technological advancement, and national legal autonomy with international copyright norms by using a doctrinal and analytical methodology.

Ultimately, this paper argues for a reimagined copyright governance framework in India — one that embeds AI accountability, data ethics, and equitable recognition of human creative contribution within its legislative and policy structures. Such reform is crucial to ensuring that India's copyright ecosystem evolves as both technologically adaptive and ethically grounded in the digital age.

Keywords: *Copyright Governance, Artificial Intelligence, Authorship and Ownership, Ethical Challenges, Indian Copyright Law.*

I. INTRODUCTION

India's copyright framework has historically evolved alongside technological and cultural developments, from the Copyright Act of 1914 to the consolidated 1957 legislation and later amendments aligning with global standards such as TRIPS (Narayanan, 2018; WIPO, 2013)[3]. Yet much of this system reflects a pre-AI environment centred on human authorship and

[1]*Currently, the Author is a 2nd Year Ph.D. Research Scholar at School of Doctoral Research & Innovation (SDRI) of GLS University (Ahmedabad. The Author's Qualifications involve: B.A. (Economics), LL.B., LL.M. (Human Rights & Duties), and LL.M. (Criminal & Security Laws). She can be reached out by her email address: maitrishail@gmail.com*
[2]*Currently, the Co-Author is an Assistant Professor at the GLS University (Ahmedabad) and the Ph.D. Guide of the Author. She can be reached out by her email address: sonal.raval@glsuniversity.ac.in*
[3]*Narayanan, P. (2018). Intellectual property law. Eastern Book Company; and WIPO. (2013). Guide to the copyright and related rights treaties. World Intellectual Property Organization.*

physical dissemination (Ghosh, 2020)[4]. Generative AI disrupts these foundations by training on massive datasets—including copyrighted works—often without consent, blurring boundaries between originality, authorship, and automated reproduction (Samuelson, 2023)[5]. As digital platforms reshape creation and distribution, intersections with privacy, data protection, and platform regulation intensify (Cohen, 2019)[6]. Consequently, copyright "governance" must extend beyond law to include institutional, ethical, and algorithmic accountability frameworks (Floridi & Cowls, 2021)[7].

1.1 Statement of the Problem:

India's copyright framework is struggling to keep pace with the accelerated development of AI technologies. Existing laws do not adequately clarify:

- whether AI-generated works receive copyright protection;
- the status of training data obtained without consent;
- the liability of platforms deploying generative AI;
- the rights of creators whose works are used for machine learning;
- the balance between innovation and creators' economic interests;
- mechanisms to ensure ethical, transparent, and accountable AI use.

This creates legal uncertainty, ethical dilemmas, and governance gaps that weaken copyright protection, hinder innovation, and expose creators and users to exploitation and opacity.

1.2 Research Questions and Hypotheses:

1.2.1 Main Research Questions:

1. How is AI transforming the understanding of authorship, originality, and creativity within Indian copyright governance?
2. Do current Indian copyright laws adequately address AI-generated works and the use of copyrighted content for machine learning?
3. What governance gaps exist in regulating AI-driven creative technologies?
4. What legal and ethical frameworks can enable a balanced approach to creativity, innovation, and rights protection?

1.2.2 Hypotheses:

- **H1:** The current Indian copyright framework is insufficient to regulate the complexities introduced by generative AI.
- **H2:** Ethical governance mechanisms—beyond statutory reform—are essential for balancing innovation with creator protection.
- **H3:** A comparative study of global models shows that hybrid governance (legal + ethical + technical) is more effective than purely legal reforms.

1.3 Objectives of the Study:

1. To examine the evolution and limitations of India's copyright governance in the digital and AI era.
2. To analyse the legal, ethical, and technological challenges posed by AI-generated content.
3. To compare India's governance deficiencies with international models such as the EU AI Act, US Copyright Office guidelines, and UK consultations.
4. To propose a balanced, ethical, and future-ready governance framework for India.

1.4 Aim of the Research:

The overarching aim is to **reimagine India's copyright governance ecosystem** by identifying policy gaps and

[4]*Ghosh, S. (2020). Copyright and emerging technologies in India. Journal of Intellectual Property Studies, 4(2), 45–68.*
[5]*Samuelson, P. (2023). Copyright's challenges in the age of generative AI. Communications of the ACM, 66(11), 20–24.*
[6]*Cohen, J. E. (2019). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.*
[7]*Floridi, L., & Cowls, J. (2021). A unified framework of five principles for AI in society. Harvard Data Science Review, 3(1), 1–15.*

proposing legal and ethical solutions that harmonise human creativity, technological innovation, and public interest in the age of Artificial Intelligence.

1.5 Methodology Adopted (Doctrinal + Analytical + Comparative):

This research adopts a **doctrinal methodology**, examining statutory provisions, case law, policy papers, and regulations governing copyright and AI in India. A **critical analytical approach** is used to interpret how these provisions apply to AI-driven challenges such as automated content creation, text-and-data mining, and platform liability. Additionally, a **comparative method** evaluates emerging frameworks in jurisdictions such as the EU, UK, and USA to draw insights for reforming India's governance architecture. Secondary sources include academic literature, government reports, WIPO documents, and technological ethics scholarship.

1.6 Scope and Limitations of the Paper:

The scope of this paper is limited to **copyright governance in India** with particular reference to AI and digital technologies. It focuses on legal, policy, and ethical issues rather than technical algorithmic design. It does not empirically assess user behaviour, economic market modelling, or technological implementation. The comparative analysis is selective, focusing on major global frameworks that provide instructive governance models. The study aims to offer conceptual and normative insights rather than empirical data or statistical modelling.

II. Conceptual and Theoretical Framework:

2.1 Meaning of "Copyright Governance" vs. "Copyright Enforcement":

Copyright governance refers to the broader institutional, policy, and normative structures that regulate the creation, ownership, dissemination, and use of creative works in society. It includes frameworks for licensing, dispute resolution, stakeholder participation, and alignment with digital economy goals (Dusollier, 2020)[8]. In contrast, copyright enforcement focuses on the legal and procedural mechanisms used to prevent and remedy infringements, such as litigation, takedowns, technological protection measures, and intermediary liability. While enforcement is reactive, governance is proactive, shaping the rules, institutions, and ethical boundaries within which copyright operates. The rise of AI has widened this distinction, demonstrating the need for governance models that move beyond punitive enforcement to systemic regulation.

2.2 Theoretical Perspectives Underpinning Copyright:

2.2.1 Utilitarian Theory:

The utilitarian justification perceives copyright as an incentive mechanism that promotes creativity and social welfare by granting exclusive rights in exchange for public access after a limited duration (Landes & Posner, 1989)[9]. The theory assumes that creators require tangible rewards to invest labour, time, and resources in producing original works.

2.2.2 Labor and Personality Theory:

Rooted in Locke's labour theory, this view posits that authors deserve rights over their creations because they invest personal effort and imprint their personality onto the work (Hughes, 1988)[10]. This theory emphasises moral rights, including the right of

[8]*Dusollier, S. (2020). Copyright law in the digital environment. Edward Elgar.*
[9]*Landes, W., & Posner, R. (1989). An economic analysis of copyright law. Journal of Legal Studies, 18, 325–363.*
[10]*Hughes, J. (1988). The philosophy of intellectual property. Georgetown Law Journal, 77, 287–366.*

attribution and integrity.

2.2.3 Public Interest Theory:

Public interest theory sees copyright as a tool to ensure societal access to knowledge, cultural development, and democratic participation (Samuelson, 1990)[11]. It stresses balancing exclusivity with access, especially in education, research, and public welfare domains.

2.3 AI's Impact on These Theoretical Justifications

AI disrupts the foundations of classical copyright theories. Utilitarian incentives weaken because AI can generate works without human creative labour, challenging the rationale for exclusive ownership. Labor-based theories struggle because AI-generated works lack human authorship and personal imprint, raising questions about originality. Public interest theory gains renewed importance as AI models rely on mass data scraping, necessitating a governance framework that ensures equitable access while preventing over-extraction of copyrighted works for training datasets (Cohen, 2019)[12]. The theoretical tensions highlight the need to reconceptualize copyright in an age where creativity is increasingly automated and data-driven.

2.4 Relevance of Ethical AI and Responsible Innovation Frameworks

Ethical AI principles—transparency, accountability, fairness, and explainability—intersect significantly with copyright governance. Responsible innovation frameworks advocate designing technologies that balance innovation with societal values and rights (Floridi & Cowls, 2019)[13]. These frameworks help ensure that AI-driven creativity respects human rights, cultural diversity, and democratic participation. Integrating AI ethics into copyright governance ensures that automated creativity does not undermine authors' moral and economic rights.

2.5 Digital Commons and the Balance Between Exclusivity and Access

The digital commons approach emphasises open access, shared knowledge, and collective innovation. Open-source and open-licensing ecosystems demonstrate how creativity can thrive through collaborative models (Benkler, 2006)[14]. In the AI era, the digital commons become crucial as datasets, pretrained models, and algorithms function as shared resources. Yet, excessive openness may conflict with copyright protection, especially when copyrighted works are used to train AI. The challenge for governance is to balance exclusivity—necessary for protecting authors—with access—necessary for innovation, research, and equitable digital development. Achieving this balance defines the future trajectory of copyright governance in India's AI-driven economy.

III. Evolution of Copyright Governance in India:

3.1 Pre-Independence and Post-Independence Copyright Regimes:

India's copyright governance evolved from colonial-era legislation to a robust post-independence statutory regime. The earliest framework emerged with the Indian Copyright Act of 1847, influenced heavily by British copyright law. Subsequent revisions aligned Indian law with developments in the UK, particularly the Copyright Act of 1911 (Narayanan, 2017)[15]. After independence, India recognised the need for an autonomous and comprehensive legislative system that addressed indigenous cultural production, leading

[11]*Samuelson, P. (1990). Copyright and public interest. Journal of Intellectual Property Law, 4, 15–31.*
[12]*Cohen, J. (2019). Between truth and power. Oxford University Press.*
[13]*Floridi, L., & Cowls, J. (2019). A unified framework of AI ethics. Minds and Machines, 29(2), 1–14.*
[14]*Benkler, Y. (2006). The wealth of networks. Yale University Press.*
[15]*Narayanan, P. (2017). Intellectual property law.*

to the enactment of the Copyright Act, 1957, which remains the principal legislation governing copyright today.

3.2 The Copyright Act, 1957 and Subsequent Amendments (1994, 2012):

The 1957 Act consolidated copyright protection across literary, dramatic, musical, artistic, and cinematographic works while establishing administrative structures such as the Copyright Office and the Copyright Board.

3.2.1 The Amendment of 1994:

The 1994 amendment modernised Indian copyright law through stronger protections for computer software, performers' rights, rental rights, and enhanced remedies against piracy. It marked India's first step toward digital-era adaptation by addressing satellite broadcasting, video piracy, and emerging technological forms of exploitation (Gopalakrishnan & Agitha, 2014).

3.2.2 The 2012 Amendment:

The 2012 amendment aligned India with the WIPO Internet Treaties, strengthened author and performer rights, enhanced royalty rights for composers and lyricists, and introduced provisions on technological protection measures (TPMs) and rights management information. The amendment also addressed disability access and made India more compliant with international standards relating to digital rights.

3.3 Influence of International Conventions:

3.3.1 Berne Convention:

India joined the Berne Convention in 1928, gaining exposure to global copyright norms such as automatic protection and national treatment. Berne's originality standard and author-centric principles continue to shape Indian jurisprudence (Ricketson & Ginsburg, 2006).

3.3.2 TRIPS Agreement:

The TRIPS Agreement (1995) introduced minimum global IP standards and compulsory enforcement obligations. For India, this accelerated legal reforms, particularly in digital enforcement, software protection, and border measures (WTO, 1995).

3.3.3 WIPO Copyright Treaty (WCT):

Although not a member of the WCT, India incorporated many of its requirements through the 2012 amendment, including TPMs and digital rights management norms, reflecting the Treaty's influence on national policy.

3.4 Role of Indian Judiciary in Shaping Copyright Jurisprudence:

3.4.1 R.G. Anand v. Deluxe Films (1978):

This landmark case established the "substantial similarity" test and clarified that copyright does not protect ideas, only their expression. The judgment remains foundational in assessing infringement claims.

3.4.2 Eastern Book Company v. D.B. Modak (2008):

The Supreme Court adopted a "modicum of creativity" standard, moving away from the sweat-of-the-brow doctrine. This decision remains highly relevant for contemporary debates on AI-generated works.

3.4.3 Other Key Decisions:

Cases such as Academy of General Education v. B. Malini Mallya and Super Cassettes v. MySpace contributed significantly to shaping doctrines around fair dealing, intermediary liability, and digital infringement.

3.5 Administrative Mechanisms: Copyright Office,

[16]*Gopalakrishnan, N. S., & Agitha, T. G. (2014). Principles of intellectual property.*
[17]*Ricketson, S., & Ginsburg, J. (2006). International copyright and neighbouring rights.*
[18]*WTO. (1995). Agreement on Trade-Related Aspects of Intellectual Property Rights.*

Board, and Appellate Bodies:

The Copyright Office administers registration, while the erstwhile Copyright Board—now replaced by the Intellectual Property Appellate Board (IPAB), and subsequently merged with commercial courts—played a crucial adjudicatory role. These bodies facilitate licensing, dispute resolution, and regulate copyright societies (Narayanan, 2017)[19].

3.6 Emerging Governance Gaps in the Digital Economy:

Despite progressive reforms, significant governance gaps persist in addressing digital piracy, online licensing, AI-generated content, text-and-data mining, and cross-border infringement. The absence of explicit AI-related provisions, limited technological enforcement capacities, and weak coordination between regulatory bodies pose challenges to effective digital copyright governance (Samuelson, 2020)[20].

IV. Artificial Intelligence and Copyright: Global and Indian Perspectives:

4.1 Overview of AI-Generated Works and Ownership Dilemmas:

AI-generated works challenge the foundational principles of copyright, which presuppose human creativity, intentionality, and originality. Generative AI models produce texts, music, and images that resemble human-authored works, raising questions regarding ownership, liability, and public-domain status (Gervais, 2020)[21]. The central dilemma is whether copyright should extend to machine outputs, and if so, who—the developer, user, or AI system—should own the rights. Many legal systems continue to rely on human authorship as a prerequisite, thereby placing AI-generated works outside traditional copyright protection.

4.2 Global Comparative Approaches (UK, EU, US, Japan):

4.2.1 United Kingdom:

The UK remains the only major jurisdiction explicitly recognizing **computer-generated works** under Section 9(3) of the Copyright, Designs and Patents Act 1988, assigning authorship to the person making the "arrangements necessary" for creation. While intended to promote innovation, critics argue that this expands artificial authorship without clear policy justification (Bently & Sherman, 2014)[22].

4.2.2 European Union:

The EU applies a strict human authorship requirement, reaffirmed in the Infopaq and Pelham decisions, where originality hinges on "the author's own intellectual creation" (Geiger et al., 2021)[23]. The EU Copyright Directive and AI Act emphasize transparency in training datasets while refraining from granting copyright to AI-generated outputs.

4.2.3 United States:

The U.S. Copyright Office maintains a firm stance that works produced autonomously by AI lack the human authorship required for copyright protection. Cases such as Thaler v. Perlmutter and decisions involving the graphic novel Zarya of the Dawn reiterate that creative human input is essential (U.S. Copyright Office, 2023)[24].

4.2.4 Japan:

Japan adopts a pragmatic innovation-centric approach.

[19]*Narayanan, P. (2017). Intellectual property law.*
[20]*Samuelson, P. (2020). Data mining, AI training, and copyright. Communications of the ACM, 63(9), 24–27.*
[21]*Gervais, D. (2020). The machine as author. Iowa Law Review, 105(5), 2053–2106.*
[22]*Bently, L., & Sherman, B. (2014). Intellectual property law.*
[23]*Geiger, C., Frosio, G., & Bulayenko, O. (2021). The EU text and data mining exceptions. IIC, 52(9), 1210–1235.*
[24]*U.S. Copyright Office. (2023). Copyright registration guidance: Works containing AI-generated material.*

While it does not grant copyright to AI-generated works, its copyright exceptions facilitate text-and-data mining (TDM) for machine learning under broad statutory allowances, enabling AI development while protecting market access (METI, 2019).

4.3 Position under Indian Law: Originality, Authorship, and Fixation Issues:

4.3.1 Originality:

Indian copyright jurisprudence follows the "modicum of creativity" standard as articulated in Eastern Book Company v. D.B. Modak (2008). AI-generated works that lack human creativity fall outside this threshold.

4.3.2 Authorship:

The Copyright Act, 1957 defines the author as a human person. Therefore, ownership cannot vest in AI, nor can a developer or user be treated as author without demonstrable creative input.

4.3.3 Fixation:

While fixation is not explicitly mandated, Indian courts consider expression in tangible form essential for subsistence. AI outputs can meet fixation requirements, but authorship and originality remain unresolved.

4.4 AI as Both Creator and Infringer:

4.4.1 AI as Creator:

AI systems can autonomously generate expressive works, but legal systems typically deny copyright protection, placing such works in the public domain by default.

4.4.2 AI as Infringer:

AI may unintentionally infringe by reproducing copyrighted materials used during training or by generating outputs resembling existing works. Liability generally falls on human users, developers, or platforms (Samuelson, 2020)[26].

4.5 Case References and Scholarly Debates

4.5.1 Key Global Cases:

Notable cases include Thaler v. Perlmutter (U.S.), Infopaq (EU), and UK decisions interpreting Section 9(3). These cases reinforce human authorship and limit copyright for AI.

4.5.2 Scholarly Debates:

Scholars debate whether AI-generated works should receive sui generis protection or remain in the public domain to enable innovation. Gervais (2020)[27] argues for transparency-based models, whereas others emphasize labour-value and personhood theories.

4.6 Data Protection, Fair Use, and Algorithmic Transparency in AI Training Datasets:

4.6.1 Data Protection:

Training datasets often include personal data, raising privacy risks and potential violations of data protection laws such as India's DPDP Act, 2023 (Kuner, 2021)[28].

4.6.2 Fair Use / Fair Dealing

India's fair dealing provisions are narrow, lacking explicit TDM exceptions. This hinders AI development and raises ambiguity around lawful data scraping.

4.6.3 Algorithmic Transparency

Opaque training datasets prevent accountability for infringement and bias. Calls for transparent AI governance frameworks are growing globally (OECD, 2019)[29].

V. Legal and Ethical Challenges in the Age of AI

5.1 Ownership vs. Public Interest in AI-Created Content

AI-generated content raises fundamental tensions between private ownership claims and the public

[26]*Samuelson, P. (2020). Data mining, AI training, and copyright. Communications of the ACM, 63(9), 24–27*
[27]*Gervais, D. (2020). The machine as author. Iowa Law Review, 105(5), 2053–2106.*
[28]*Kuner, C. (2021). Data protection in the global digital economy. International Data Privacy Law, 11(1), 1–5.*
[29]*OECD. (2019). OECD principles on Artificial Intelligence.*

interest in access, innovation, and the commons. Traditional copyright doctrine—grounded in human creativity—struggles to accommodate outputs autonomously produced by machine-learning systems (Gervais, 2020)[30]. While some argue for granting proprietary rights to incentivize AI development, others caution that doing so would expand monopolies and artificially restrict the public domain (Samuelson, 2020)[31]. In the absence of human authorship, many jurisdictions, including the U.S., favour keeping AI-only outputs unprotected, allowing society to benefit from unrestricted dissemination. For India, the challenge lies in balancing economic incentives for technology developers with equitable access to knowledge resources.

5.2 Accountability and Attribution in AI-Involved Creativity

As AI systems increasingly participate in creative processes—generating text, images, or music—questions arise about who should be credited and held accountable for the results. Human creators may contribute prompts, curation, or post-editing, but the degree of creativity required to qualify for authorship remains ambiguous (Bently & Sherman, 2014)[32]. Attribution becomes further complicated when outputs replicate or transform copyrighted works in training datasets. Creating a framework for shared or layered authorship, alongside transparent disclosure requirements, is essential to preventing misappropriation and ensuring ethical creative collaboration between humans and AI.

5.3 Transparency, Bias, and Ethical AI Governance

AI systems rely on vast datasets that often include unlicensed copyrighted works, personal data, and culturally biased representations. Lack of transparency about training data sources prevents effective copyright enforcement and limits user trust (Cohen, 2019)[33]. Algorithmic bias raises additional ethical concerns, particularly when generative models perpetuate harmful or stereotypical content. Ethical AI governance principles—such as those proposed by the OECD—call for transparency, accountability, fairness, and robust risk assessments (OECD, 2019)[34]. Implementing these principles within India's copyright and digital governance regime is essential to mitigating discriminatory outputs and ensuring rights-respecting technological development.

5.4 Intersection with Moral Rights and Right to Privacy

AI training processes involving large-scale data scraping directly implicate moral rights and privacy interests. Authors' moral rights to attribution and integrity may be undermined when their works are subsumed into opaque datasets that generate derivative or distorted content (Geiger et al., 2021)[35]. Privacy risks emerge when AI models ingest personal data—including photos, communications, or biometric identifiers—without meaningful consent. The overlap between copyright governance and privacy regulation requires a harmonised, cross-sectoral approach to protect individual dignity and prevent exploitative data practices.

5.5 The Challenge of Cross-Border Digital Enforcement

[30]*GGervais, D. (2020). The machine as author. Iowa Law Review, 105(5), 2053–2106.*
[31]*Samuelson, P. (2020). Data mining, AI training, and copyright. Communications of the ACM, 63(9), 24–27.*
[32]*Bently, L., & Sherman, B. (2014). Intellectual property law.*
[33]*Cohen, J. (2019). Between truth and power: The legal constructions of informational capitalism.*
[34]*OECD. (2019). OECD principles on artificial intelligence.*
[35]*Geiger, C., Frosio, G., & Bulayenko, O. (2021). The EU text and data mining exceptions. IIC, 52(9), 1210–1235.*

The global and decentralised nature of digital platforms makes copyright enforcement across jurisdictions increasingly complex. AI technologies trained in one country may generate infringing content accessible worldwide, while cloud-based service architectures obscure the location of data and computation. Differences in national copyright laws, intermediary liability regimes, and AI regulatory frameworks hinder harmonised enforcement (Kuner, 2021). India faces additional challenges due to limited technological capacity and inconsistencies in cross-border cooperation mechanisms, highlighting the need for robust international partnerships and digital enforcement tools.

5.6 Ethical Dilemmas of Algorithmic Creativity — Authorship vs. Automation

At the heart of AI-driven creativity lies a deeper philosophical and ethical tension: whether creative agency can be attributed to machines. Some view algorithmic creativity as an extension of human intention, while others argue that automation lacks consciousness, intentionality, and moral responsibility (Floridi & Sanders, 2004). Excessive reliance on AI risks diminishing human creative value and displacing traditional artistic labour. Conversely, restricting AI involvement may impede innovation. Crafting an ethical middle path requires reinforcing human oversight, preserving authorship as a fundamentally human domain, and developing governance frameworks that recognise AI as a tool—not an autonomous creator.

VI. Policy Gaps and Institutional Challenges in India

6.1 Absence of AI-Specific Legal Recognition in Copyright Law

India's Copyright Act, 1957 does not explicitly address artificial intelligence or AI-assisted creativity, resulting in doctrinal uncertainty regarding authorship, fixation, and liability. The statute's human-centric definitions of "author" and "original work" fail to accommodate emerging forms of machine-generated outputs (Bently & Sherman, 2014). With AI models increasingly trained on large scraped datasets—including copyrighted works—this absence generates ambiguity about licensing, infringement, and fair use-like exceptions. Comparative jurisdictions such as the U.S. and EU have issued clear regulatory or administrative guidance, whereas India lacks a harmonized interpretive framework, weakening legal predictability for creators and technology developers (Gervais, 2020).

6.2 Weakness in Digital Enforcement Infrastructure (e.g., Intermediary Liability)

While India introduced intermediary liability reforms under the Information Technology Rules (2021), enforcement remains fragmented. Overbroad obligations, inadequate clarity on safe-harbour provisions, and inconsistent takedown procedures hinder effective governance (Chawla, 2022). Platforms struggle with compliance burdens amid unclear expectations for monitoring AI-generated or infringing content. Furthermore, the absence of dedicated copyright-focused digital enforcement units limits India's capacity to address large-scale online infringement, automated scraping, and rapid content dissemination.

6.3 Gaps in Data Governance and Copyright Licensing

[36]*G Kuner, C. (2021). Data protection in the global digital economy. International Data Privacy Law, 11(1), 1–5.*
[37]*Floridi, L., & Sanders, J. (2004). On the morality of artificial agents. Minds and Machines, 14(3), 349–379.*
[38]*Bently, L., & Sherman, B. (2014). Intellectual property law.*
[39]*Gervais, D. (2020). The machine as author. Iowa Law Review, 105(5), 2053–2106.*
[40]*Chawla, A. (2022). Intermediary liability in India's digital ecosystem. Indian Journal of Law and Technology, 18(2), 45–62.*

India's Digital Personal Data Protection Act (2023) primarily focuses on privacy but does not address non-personal data flows relevant to AI training and copyright licensing. The lack of a comprehensive data governance framework results in inadequate regulatory oversight of dataset sourcing, consent protocols, and cross-border data flows (Kuner, 2021). Licensing mechanisms for text-and-data mining (TDM)—integral for training foundation models—remain underdeveloped, creating uncertainty for tech companies and limiting creators' ability to monetise digital uses of their works. These gaps hinder both innovation and rights protection.

6.4 Lack of Transparency and Coordination Between Administrative Bodies

Copyright governance in India is shared across multiple institutions—Copyright Office, IPAB (now merged into High Courts), Ministry of Electronics and IT (MeitY), and the Department for Promotion of Industry and Internal Trade (DPIIT). However, coordination is weak, resulting in inconsistent policy positions on platform regulation, algorithmic accountability, and data governance. Administrative opacity, limited public consultation, and inadequate technical capacity further undermine trust and policy coherence (Cohen, 2019).

6.5 Challenges for Creators, Platforms, and Users

6.5.1 Challenges Faced by Creators

Creators encounter widespread unauthorized scraping of their works for AI training, absence of clear compensation mechanisms, and limited knowledge of digital licensing tools. They also struggle with platform-driven revenue models that undervalue creative labour (Samuelson, 2020). The lack of statutory protections for AI-assisted authorship further complicates ownership claims.

6.5.2 Challenges Faced by Platforms

Platforms face unclear intermediary obligations, ambiguous safe-harbour protections, and unpredictable enforcement actions. They must manage large volumes of AI-generated content without clear regulatory guidelines. Inadequate coordination between copyright and IT regulators increases compliance uncertainties.

6.5.3 Challenges Faced by Users

Users confront opaque algorithms, varied takedown procedures, and limited access to lawful digital content due to licensing inefficiencies. Over-enforcement risks chilling legitimate speech and creativity, while under-enforcement enables misinformation and piracy (Electronic Frontier Foundation, 2015).

6.6 Stakeholder Perspectives: Authors, Tech Companies, Regulators, and Academia

Authors demand stronger rights, transparent consent mechanisms, and fair remuneration for AI-related uses of their works. Tech companies seek predictable regulation, flexible licensing models, and innovation-friendly exceptions. Regulators focus on balancing public interest, market competition, and digital sovereignty, yet face capacity constraints. Academia emphasizes evidence-based policy, advocating interdisciplinary frameworks that integrate copyright, data ethics, and AI governance. These differing viewpoints highlight the need for an adaptive, multi-stakeholder governance model capable of addressing India's technological and cultural diversity.

[41]*Kuner, C. (2021). Data protection in the global digital economy. International Data Privacy Law, 11(1), 1–5.*
[42]*Cohen, J. (2019). Between truth and power: The legal constructions of informational capitalism.*
[43]*Samuelson, P. (2020). Data mining, AI training, and copyright. Communications of the ACM, 63(9), 24–27.*
[44]*Electronic Frontier Foundation. (2015). Manila principles on intermediary liability.*

VII. Comparative Study: Lessons from Global Copyright Governance Models:

7.1 EU AI Act and Copyright Directive:

The European Union has pioneered a multilayered regulatory approach to artificial intelligence and digital copyright. The EU AI Act (2024) establishes risk-based governance obligations, including transparency duties for generative AI systems and requirements to disclose training data sources (European Parliament, 2024). In parallel, the EU Copyright Directive (2019) introduced text-and-data mining (TDM) exceptions while preserving rights-holder opt-outs (Geiger, Frosio, & Bulayenko, 2021). Together, these instruments form a coherent framework that balances innovation with strong authorial rights. Importantly, they mandate platform accountability and algorithmic explainability, creating a structured environment for licensing data used in AI training. For India, the EU's approach demonstrates the value of harmonizing AI-specific obligations with copyright rules, ensuring that digital innovation progresses without undermining artistic and cultural rights.

7.2 UK Approach to Computer-Generated Works:

The United Kingdom takes a distinctive stance on AI-related creativity. Under Section 9(3) of the Copyright, Designs and Patents Act (CDPA) 1988, computer-generated works (CGWs) can receive copyright protection despite the absence of a human author, with rights vested in the person undertaking "arrangements necessary for the creation of the work." While praised for legal pragmatism, this approach faces criticism for granting excessive proprietary control over automated outputs (Bently & Sherman, 2014). Recent consultations have signalled hesitancy in expanding CGW rights, noting potential risks to market competition and access. The UK model illustrates both the regulatory flexibility and challenges in defining authorship in highly automated contexts. India can learn from the UK's debates by avoiding automatic copyright for AI-generated works and insisting on a human-centric authorship threshold.

7.3 U.S. Copyright Office Guidance on AI-Authored Content

The United States offers a contrasting model grounded in a strict requirement of human authorship. In highly publicized decisions such as Zarya of the Dawn and Thaler v. Perlmutter, the U.S. Copyright Office and courts held that copyright cannot subsist in works generated autonomously by AI (U.S. Copyright Office, 2023). However, AI-assisted works may be protected if humans contribute creative selection, arrangement, or modification. The U.S. model prioritizes doctrinal consistency with long-standing originality jurisprudence while providing clear disclosure requirements when submitting works involving AI. This approach provides legal certainty and prevents monopolization of machine-generated content, offering a practical template for India to emulate.

7.4 Singapore's IP Strategy 2030 and Digital Licensing Systems

Singapore's IP Strategy 2030 promotes a forward-looking regulatory ecosystem emphasizing digital licensing, innovation enablement, and cross-border interoperability (Intellectual Property Office of Singapore [IPOS], 2021). The country's AI Verify

[45]*European Parliament. (2024). EU Artificial Intelligence Act.*
[46]*Geiger, C., Frosio, G., & Bulayenko, O. (2021). The EU text and data mining exceptions. IIC, 52(9), 1210–1235.*
[47]*Bently, L., & Sherman, B. (2014). Intellectual property law.*
[48]*U.S. Copyright Office. (2023). Copyright registration guidance: Works containing AI-generated material.*
[49]*Intellectual Property Office of Singapore. (2021). Singapore IP Strategy 2030.*

framework encourages transparent, ethical AI deployment, while IPOS promotes efficient licensing of copyrighted content through automated rights-management systems. Singapore's integration of technology-neutral IP governance with strong innovation incentives demonstrates how small jurisdictions can achieve global leadership in digital copyright management. This model highlights the importance of administrative efficiency, digital rights registries, and coordinated regulatory strategies.

7.5 Implications for India: Adaptive Governance, Innovation Facilitation, and Rights Protection:

A comparative review reveals valuable lessons for India's evolving copyright landscape. The EU's integrated approach underscores the necessity of harmonizing copyright, AI governance, and data regulation; the U.S. model offers clarity through a strict human authorship standard; the UK provides insights into both the utility and pitfalls of protecting computer-generated works; and Singapore demonstrates the advantages of technologically adaptive, innovation-oriented governance. For India, the way forward lies in adaptive governance that avoids over-regulation while enabling experimentation; innovation facilitation through licensing reforms, TDM permissions, and digital rights infrastructure; and strong rights protection via human-centric authorship, transparency obligations for AI developers, and efficient platform liability mechanisms. Drawing on global best practices, India can craft a coherent framework that safeguards creators while catalysing a competitive digital economy.

VIII. Re-Imagining Copyright Governance in India: A Way Forward:

8.1 Reinterpreting Originality and Authorship in the AI Context:

The emergence of generative artificial intelligence has disrupted classical notions of authorship and originality embedded in Indian copyright law. Under the Copyright Act, 1957, originality requires skill, judgment, and labour, while authorship presupposes human creativity (Bently & Sherman, 2014). However, AI systems produce outputs through algorithmic processing of pre-existing datasets, complicating questions of who—if anyone—owns such works. International scholarship increasingly favours a "human-centric contribution test," where copyright subsists only if a human exercises creative control over the prompt design, curation, or refinement (Gervais, 2020). India must adopt a similar interpretive framework, clarifying that AI-generated works without significant human intervention remain in the public domain. This approach ensures doctrinal coherence while preventing over-expansion of rights that could hinder innovation and access.

8.2 Establishing a "Digital Copyright Governance Authority":

Given the complexity of digital ecosystems, India requires a specialized Digital Copyright Governance Authority (DCGA) to complement the existing Copyright Office. The proposed authority would oversee algorithmic transparency, platform intermediary obligations, collective licensing mechanisms, and dispute resolution involving digital works. Drawing inspiration from the EU's Digital Services Act and Singapore's IMDA model, the DCGA would operate as a cross-disciplinary body with technological, legal, and economic expertise (Cohen,

[50]*Bently, L., & Sherman, B. (2014). Intellectual property law.*
[51]*Gervais, D. (2020). The machine as author. Iowa Law Review, 105(5), 2053–2106.*

2019)[52]. Such an institution would bridge regulatory gaps and ensure dynamic governance aligned with technological change.

8.3 AI Accountability Mechanisms: Algorithmic Audits and Ethical Codes:

To ensure responsible AI creativity, India must integrate mandatory algorithmic audits, fairness assessments, and model documentation norms. Ethical codes—such as the OECD AI Principles—emphasize transparency, explainability, and accountability (OECD, 2019)[53]. Copyright governance frameworks must therefore require AI developers and digital platforms to disclose training data sources, licensing practices, and potential copyright risks. This promotes traceability and facilitates equitable attribution while reducing unlawful scraping of copyrighted materials.

8.4 Integration of Copyright with Data Protection and Digital Economy Policies:

The increasing overlap between data protection, competition law, and copyright necessitates a coherent, cross-sectoral governance architecture. India's Digital Personal Data Protection Act (2023) and proposed Digital India Act can complement copyright reforms by regulating data flows, platform responsibilities, and user rights. A unified policy framework would prevent siloed regulation, promote interoperability, and support fair data-driven innovation (Kuner, 2021)[54]. Integrating copyright with broader digital economy policies strengthens consumer protection and fosters a rights-respecting digital environment.

8.5 Proposal for Model Statutory Amendments (Copyright Act, 1957):

Key reforms should include: (a) statutory recognition of human-AI collaborative authorship; (b) explicit exclusion of fully automated AI-generated works from copyright; (c) mandatory disclosure of AI training data sources; (d) safe-harbour reforms balancing innovation with rights-holder protections; and (e) updated definitions of "communication to the public" and "technological protection measures." These amendments would modernize the Act while aligning India with global developments.

8.6 Proposal for Takedown SOPs and Digital Content Governance Guidelines:

A model takedown framework should mandate time-bound responses, clear notices, due-process safeguards, counter-notice options, and transparency reporting. Platforms must also maintain databases of repeat infringers while ensuring protection against arbitrary censorship. A rights-respecting takedown SOP aligns with international best practices such as the Manila Principles (Electronic Frontier Foundation, 2015)[55].

8.7 Adoption of Open Licensing and Fair Remuneration Frameworks:

To balance access and incentives, India should promote open licensing models—including Creative Commons—alongside equitable remuneration schemes for creators whose works inform AI training. Collective management organizations may facilitate standardized licensing for large-scale text-and-data mining (Samuelson, 2020)[56].

8.8 Need for International Cooperation and Harmonization:

Finally, cross-border cooperation is vital, given the global nature of AI models and digital infringement.

[52]*Cohen, J. (2019). Between truth and power: The legal constructions of informational capitalism.*
[53]*OECD. (2019). OECD principles on artificial intelligence.*
[54]*Kuner, C. (2021). Data protection in the global digital economy. International Data Privacy Law, 11(1), 1–5.*
[55]*Electronic Frontier Foundation. (2015). Manila principles on Intermediary Liability.*
[56]*Samuelson, P. (2020). Data mining, AI training, and copyright. Communications of the ACM, 63(9), 24–27.*

India must actively engage in WIPO dialogues, support harmonized AI-copyright standards, and push for fair global licensing frameworks. International alignment ensures legal certainty and strengthens India's position in the global digital economy.

IX. Conclusion and Recommendations:

India stands at a pivotal moment in reimagining its copyright governance framework as Artificial Intelligence (AI) transforms creative, cultural, and informational ecosystems. Three major shifts shape this new landscape: (i) the exponential rise of AI systems dependent on vast datasets containing copyrighted works and personal information; (ii) the legal mismatch between traditional copyright doctrines and AI-generated outputs; and (iii) profound ethical challenges at the intersection of IP, data governance, and algorithmic decision-making. Collectively, these developments reveal that India's copyright regime—largely rooted in the Copyright Act of 1957—requires urgent modernization to remain effective and globally competitive.

The study highlighted a widening gap between technological innovation and legal-ethical safeguards. The Indian framework lacks clarity on text-and-data mining (TDM), fair dealing boundaries, and the ownership status of AI-generated works. As AI models increasingly scrape copyrighted works, unresolved doctrinal tensions around originality and authorship heighten conflicts between rightsholders and developers. This tension—between promoting innovation and protecting human creativity—emerged as a central theme.

Indian jurisprudence assumes human authorship and human-centred creativity, creating a vacuum for AI-generated outputs. Meanwhile, global jurisdictions diverge: the EU leans toward TDM exceptions with opt-out provisions; the US denies copyright protection for non-human authorship; and the UK preserves a statutory regime recognizing computer-generated works. India must therefore chart a context-specific, balanced path that safeguards authors, regulates developers, and promotes innovation.

Ethical issues further reinforce the need for integrated governance. Privacy, fairness, bias, and transparency concerns are inseparable from AI-related copyright disputes. Black-box AI systems, potential discrimination in datasets, and excessive surveillance through digital enforcement highlight the limits of a purely legalistic approach. Effective digital governance must therefore incorporate ethical AI principles, platform regulation, and data protection.

India's enforcement ecosystem also faces structural challenges in addressing deepfakes, synthetic media, and cross-border infringement. Existing takedown mechanisms under the IT Act, 2000 and Intermediary Guidelines, 2021 remain inconsistent and opaque. Earlier sections of this study argued for a specialized Digital Copyright Governance Authority (DCGA) to streamline dispute resolution, platform compliance, algorithmic audits, and licensing.

AI's dual role—as both a disruptor and an enabler of creativity—underscores the urgency of adaptive governance. Without reform, India risks increased litigation, market concentration, and disproportionate harm to independent creators.

Key Recommendations

1. **Reinterpret Originality and Authorship:** Adopt a hybrid authorship model requiring disclosure of AI involvement, recognizing human input in AI-assisted works, and denying exclusive rights in fully autonomous AI outputs. Clarifying TDM exceptions is essential.
2. **Establish a Digital Copyright Governance Authority (DCGA):** A specialized regulator should oversee algorithmic audits, TDM licensing, dispute resolution, and ethical AI guidelines, complementing existing bodies.
3. **Integrate Copyright, Data Protection, and Digital Market Policies:** Harmonize the Copyright Act, the Digital Personal Data Protection Act, and forthcoming digital market regulations.
4. **Amend the Copyright Act, 1957:** Define AI-assisted and AI-generated works, create TDM exceptions with opt-outs, mandate ethical dataset use, and enable algorithmic transparency for affected creators.
5. **Transparent Takedown SOPs:** Standardized, proportionate, and fair takedown processes with human oversight must guide platform accountability.
6. **Promote Open Licensing and Fair Remuneration:** Expand open datasets and ensure fair compensation when copyrighted works train commercial AI models.
7. **Strengthen International Cooperation:** Pursue harmonized global standards and cross-border licensing through WIPO, WTO, and G20 platforms.

Ultimately, India's future lies in creating a governance model that is adaptive, ethical, transparent, and innovation-friendly—one that ensures human creativity and AI coexist productively within a rights-respecting digital ecosystem.

BALANCING PRIVACY AND PUBLIC INTEREST: THE EMERGING LANDSCAPE OF THE RIGHT TO BE FORGOTTEN IN INDIA

Junaid Malika*

Mohammad Nasir*

ABSTRACT

The digital environment has redefined the contours of privacy by enabling the continuous creation, retention, and dissemination of personal data across global networks. In this setting, the Right to be Forgotten (RTBF) has emerged as a significant legal doctrine aimed at restoring individual autonomy over personal information that has become outdated, irrelevant, or disproportionately harmful. Recognized most prominently under Article 17 of the European Union's General Data Protection Regulation, RTBF represents a shift toward safeguarding informational privacy in an era characterized by digital permanence and unrestricted data visibility. Its evolution reflects a broader effort to reconcile individual dignity with competing interests such as freedom of expression, public access to information, and technological limitations inherent in online data management.

In India, the legal recognition of RTBF is at a formative stage. Although the Supreme Court's judgment in Justice K.S. Puttaswamy v. Union of India affirmed privacy as a fundamental right, explicit statutory provisions addressing RTBF remain absent. Judicial decisions have adopted a context-driven approach, highlighting doctrinal tensions between privacy, open justice, and constitutional freedoms. The enactment of the Digital Personal Data Protection Act, 2023, introduces mechanisms for data correction and erasure but stops short of codifying RTBF, leaving uncertainties regarding scope, enforceability, intermediary obligations, and cross-border compliance.

This study examines the conceptual foundations, historical evolution, and global regulatory approaches to RTBF, with a specific focus on its emerging trajectory in India. Through doctrinal analysis of statutes, case law, and policy documents, it evaluates the normative and practical challenges in implementing RTBF within a complex constitutional framework. The research aims to identify legal gaps and propose structured reforms to support a balanced model that protects individual privacy while upholding transparency, free expression, and democratic accountability.

I. INTRODUCTION

In the digital age, where personal information is akin to a digital footprint etched in stone, the Right to be Forgotten (RTBF) emerges as a crucial safeguard of individual privacy. As Princess Margaret lamented, "I have as much privacy as a goldfish in a bowl," reflecting the pervasive nature of modern surveillance and data retention. This sentiment underscores the urgent need for legal mechanisms that empower individuals to control their digital identities and mitigate the long-term consequences of online information.

RTBF finds its roots in the broader evolution of privacy

**Department of Law, Aligarh Muslim University, Aligarh-202002, U.P., INDIA*

[1] *Paul Lambert, The Right to Be Forgotten: Interpretation and Practice (Bloomsbury Professional 2019).*

[2] *Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton University Press 2011).*

[3] *Naman Khatwani, "The Right to Be Forgotten: Incorporation in India" (2020) 4 Journal of Intellectual Property Studies 57.*

[4] *Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India 2021).*

rights. Historically, privacy has been synonymous with the right to be left alone, shielding individuals from unwanted intrusion. However, as the digital landscape expanded, so did the need for a nuanced approach to privacy. The European Union (EU) has been at the forefront of formalizing RTBF through legislative instruments like the General Data Protection Regulation (GDPR). This regulation grants individuals the right to request the deletion of personal data under certain circumstances, recognizing the need to balance individual privacy with public access to information.Philosophically, RTBF is grounded in principles of autonomy and dignity, aiming to empower individuals to shape their online narratives and protect their reputations. It distinguishes itself from other privacy rights, such as the right to erasure, by specifically addressing the accessibility and permanence of personal data in the digital sphere. This distinction is crucial as it navigates the complexities of digital memory and the implications of online information on personal and professional lives.

The digital revolution has fundamentally transformed the way information is created, stored, disseminated, and accessed. In today's interconnected world, the internet serves as a vast repository of data, much of which pertains to individual identities, past activities, legal records, news coverage, and social footprints. Against this backdrop, the emergence of the concept of the "Right to be Forgotten" (RTBF) reflects a growing recognition of the need for individuals to have some degree of control over their digital identities. The Right to be Forgotten refers to an individual's right to request the deletion or delisting of personal data from internet platforms so that such data is no longer available to the public. The central idea behind this right is the protection of an individual's privacy and dignity, especially when the data in question is no longer necessary, relevant, accurate, or serves a legitimate public interest. It is rooted in the broader realm of data protection and informational privacy, aiming to provide individuals with autonomy over their personal information and a chance to move on from their past without it haunting them perpetually in the digital space.

The Right to be Forgotten is not an absolute right; rather, it is a qualified and context-dependent claim, subject to limitations such as freedom of expression, the right to information, and public interest. It typically applies to situations where outdated, irrelevant, or inaccurate personal data remains publicly accessible and causes harm to the individual concerned. In legal and policy discourses, the RTBF is closely associated with the broader right to privacy and the concept of informational self-determination, which emphasizes that individuals should have the agency to determine how their personal data is collected, used, stored, and shared. While the terminology "Right to be Forgotten" is relatively recent, the underlying principles trace back to older philosophical and legal notions of human dignity, the right to reputation, and the possibility of social reintegration after mistakes, especially in criminal and civil matters.

This ruling marked a significant turning point in the global conversation about protecting personal data and digital privacy. It established the RTBF as a legally binding right in the EU, contingent on weighing it

[5]Ceera, "Transparency, Good Governance and the Right to Be Forgotten", National Law School of India University,Bangalore, April 29, 2024, available at: https://ceerapub.nls.ac.in/transparency-good-governance-and-the-right-to-be-forgotten (last visited on Mar 24, 2024)
[6]Duggal Pavan, Law Relating to Data Protection and Privacy 134(Universal Law Publishing, 2nd Edition, 2020.)
[7]Justice B.N. Srikrishna Committee, "Report of the Committee of Experts on Data Protection Framework for India"229-240 Ministry of Electronics and Information Technology (MeitY), Government of India, New Delhi (April, 2018).

against other essential rights, including the public's right to information and freedom of speech. Following this ruling, the General Data Protection Regulation (GDPR), which went into effect in May 2018, was amended by the European Union to explicitly recognize the RTBF in Article 17. Under certain conditions, such as when the data is no longer required, the subject withdraws consent, or the processing is illegal, people have the right to have their personal data deleted, according to Article 17, "Right to Erasure." The GDPR lays forth the rights, conditions, and exceptions, as well as the procedures for implementing them. It has established itself as a global standard for privacy legislation in other countries, offering a thorough and enforceable framework for safeguarding digital privacy[8].

In the Indian context, the discussion on the Right to be Forgotten is of relatively recent origin but has gained significant momentum following the Supreme Court's historic verdict in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), wherein the right to privacy was declared a fundamental right under Article 21 of the Constitution. In this case, the apex court emphasized informational privacy as a crucial aspect of personal autonomy, thereby opening the door for rights like RTBF to gain recognition. While the Court did not specifically address RTBF, the broad interpretation of privacy rights has laid the constitutional foundation for its future recognition. The Court noted that privacy includes the right to control the dissemination of personal information and that individuals must have the autonomy to decide what information about them enters the public sphere[9].

Despite the legislative uncertainty, Indian courts have begun to address RTBF claims through judicial interpretation. In **Jorawer Singh Mundy v. Union of India**[10] , the Delhi High Court acknowledged the reputa-tional harm caused to an individual whose acquittal was not reflected in publicly accessible online legal records. Similarly, in **X v. Union of India**[11] , the Karnataka High Court granted relief to a woman who sought to remove her name from online court judgments related to a matrimonial dispute that had been settled amicably. In contrast, the Gujarat High Court in **Dharmraj Bhanushankar Dave v. State of Gujarat**[12] declined to grant relief on the grounds that court judgments are public records and must remain accessible for transparency. These decisions reflect the evolving nature of Indian jurisprudence in this area and the judiciary's efforts to strike a balance between privacy and openness[13].

Meaning of Right to be Forgotten:

In the realm of data protection and privacy rights, the Right to be Forgotten (RTBF) is a relatively new yet important concept, particularly in light of the ever-evolving digital world. Fundamentally, the right refers to a person's ability to request that personal information be deleted from databases, search engines, and public platforms when it is no longer required, pertinent, or accurate, or when its continued availability violates their right to privacy and dignity. Following the historic ruling in Google Spain SL v. Agencia Española de Protección de Datos (AEPD)[14] by the Court of Justice of the European Union (CJEU),

[8]*Uppaluri Ujwala, Information Technology Law and Practice 78 (LexisNexis, 1st Edition, 2013).*
[9]*Arjun Kharpal, "Why the Right to be Forgotten is Controversial" 15 Journal of Cyber Law 53(2017).*
[10]*2021 SCC Online Del 2306.*
[11]*2017 SCC Online Kar 424.*
[12]*2015 SCC Online Guj 6148.*
[13]*K.K. Singh, Cyber Laws: A Guide for Indian Lawyers 136(Universal Law Publishing, New Delhi, 4thedn., 2021).*
[14]*EU:C: 2014:317.*

which established that people could request that search engines remove links that contained personal information that was "inadequate, irrelevant, or excessive" in relation to the purposes for which it was processed, the idea gained significant traction in European jurisprudence. Thus, the RTBF exemplifies the idea that people need to have control over their personal information online, so that damaging or outdated material doesn't follow them around forever.

The meaning of this right is intrinsically connected to the broader right to privacy, which is recognized as a fundamental right under Article 21 of the Constitution of India following the Supreme Court's judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India. In the Indian context, the RTBF is understood as a facet of informational privacy, where individuals have the right to restrict or prevent the continued disclosure of their personal information, especially when it is no longer serving any legitimate public purpose. This does not necessarily mean erasing historical facts but rather ensuring that such facts are not unnecessarily linked to an individual's identity in a way that causes undue harm. The focus is on striking a balance between the right to privacy and other competing rights, such as freedom of expression, the right to information, and public interest.

Origin and Development:

The Right to be Forgotten (RTBF), though often considered a modern construct of the digital era, finds its conceptual roots in long-standing legal and philosophical notions of privacy, dignity, and control over personal information. The idea that individuals should have the ability to "erase" traces of their past, or at least limit their public accessibility, existed in various forms long before the advent of the internet. In traditional societies, personal histories and mistakes faded naturally over time because memory was short-lived and information dissemination was limited to interpersonal communication or localized records. However, with the digital revolution and the internet's capacity for global, instant, and indefinite retention of data, the natural process of societal forgetting has been replaced by what scholars describe as "digital permanence." This permanence necessitated a formal legal recognition of a right that could counterbalance the ever-expanding reach and permanence of personal data in cyberspace.

The 2014 landmark ruling in Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González by the Court of Justice of the European Union (CJEU) marked a turning point in the legal evolution of RTBF. The dispute began when Spanish national Mario Costeja González requested that links to old auction notices regarding his long-since-paid social security obligations be removed from Google search results. Search engines are "data controllers," according to the CJEU, and are required to remove links to personal information that are "inadequate, irrelevant, or excessive" in relation to the processing goals upon a legitimate request from the subject. This ruling significantly impacted global data protection standards by transforming RTBF from an intangible privacy concern into an enforceable legal right within the EU. The General Data Protection Regulation (GDPR) officially codified the RTBF in Article 17 after this ruling, and it went into force on May 25, 2018. When personal data is no longer needed, the permission for its processing is revoked, it is handled

[15]*Subramanian, Ramesh, et.al. (Eds.), The Global Flow of Information: Legal and Political Perspectives 239 (NYU Press, New York, 1stedn., 2011).*
[16]*Supra Note 3.*
[17]*Anirudh Rastogi, Cyber Law: Law of Information Technology and Internet 218-221(LexisNexis, Gurgaon, 2ndedn., 2020).*

illegally, or it is required by law, Article 17 expressly gives people the right to have it erased without undue delay. To safeguard freedom of speech, adherence to legal requirements, and the public interest in fields such as public health, scientific research, or historical preservation, the GDPR also acknowledges exceptions. The RTBF's legal structure was distinguished by this harmony between conflicting rights and privacy.

Instead of clear legislative recognition, judicial interpretation has been the main force behind the establishment of RTBF in India. The Supreme Court's nine-judge panel ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) recognized the Right to Privacy as a basic right under Article 21 and provided the constitutional basis for the RTBF. The ruling recognized informational privacy and the need for people to regulate the sharing of their personal information, even if it did not specifically address RTBF. This acknowledgment made it possible for Indian courts to take RTBF into account in later instances.

The first significant Indian case discussing RTBF was Dharamraj Bhanushankar Dave v. State of Gujarat where the petitioner sought removal of a judgment acquitting him from online legal databases to protect his reputation. The Gujarat High Court rejected the plea, citing the importance of public access to court records. Later, in K.S. Puttaswamy v. Union of India the Supreme Court's privacy ruling indirectly strengthened RTBF claims. More recently, in Jorawar Singh Mundy v. Union of India , the Delhi High Court ordered the removal of a judgment from online platforms after an acquittal in a criminal case, recognizing the potential harm to the petitioner's career prospects. Several other High Court rulings, including from Kerala, Karnataka, and Orissa, have also referred to RTBF principles, though with differing outcomes depending on the balance between privacy and the public's right to information.

I. STATEMENT OF THE PROBLEM

In an era dominated by digital interactions and pervasive data collection, the advent of the internet and its technological advancements have revolutionized how personal information is accessed, stored, and utilized. This digital transformation has ushered in unprecedented conveniences and opportunities for communication and innovation. However, it has also raised profound concerns about privacy and data protection. Personal data, once freely exchanged for ostensibly free services, now constitutes a valuable commodity subjected to widespread surveillance and monetization.Amidst this backdrop, the Right to be Forgotten (RTBF) concept has emerged as a pivotal legal and ethical issue. RTBF, rooted in principles of individual autonomy and privacy, grants individuals the right to request the removal of their data from online platforms and search engine results. While legislation such as the General Data Protection Regulation (GDPR) in Europe aims to safeguard these rights, the implementation and enforcement of RTBF face significant challenges. These challenges include balancing the right to privacy with competing interests such as freedom of expression, ensuring effective compliance across jurisdictions, and addressing technological complexities in data deletion and storage.

II. RESEARCH QUESTIONS

[18]*David Erdos, Data Protection and the Open Society: Privacy Rights and Democracy in the Information Age 278 (Hart Publishing, Oxford, 1stedn., 2020).*
[19]*2015 SCC Online Guj 2019*
[20]*AIR 2017 SC 4161*
[21] *2021 SCC Online Del 2306*

1. How has the concept of the Right to Be Forgotten (RTBF) evolved historically, and what key milestones have contributed to its development as a recognized legal right?

2. What is the scope and definition of RTBF, and how does it differ from other privacy rights within various legal and philosophical frameworks?

3. How has the European Union's GDPR, particularly Article 17, influenced the adoption and implemen tation of RTBF in non-EU countries?

4. In what ways have different international jurisdictions, such as the United States, Latin American, and Asian countries, approached RTBF, and how do these approaches vary from the European model?

5. What difficulties and disputes come up when attempting to strike a balance between the RTBF and other essential rights, such as the right to information and freedom of expression?

6. What technical challenges exist in the implementation of RTBF, particularly regarding data permanence on the internet and the role of search engines?

III. RESEARCH METHODOLOGY

This study employs a primarily doctrinal and analytical research methodology. The doctrinal approach is characterized by an in-depth examination of relevant case law, legislation, and academic literature. This method enables a comprehensive understanding of existing legal principles, frameworks, and interpretations within the field under investigation. Through systematic analysis, the research explores how legal doctrines are established, maintained, and interpreted over time, shedding light on both the foundations and nuances of pertinent legal issues.

This study primarily relies on secondary sources of data and employs a doctrinal research methodology to critically examine the laws related to the Right to Be Forgotten (RTBF) in India and the challenges associated with their implementation. The research involves an in-depth analysis of constitutional provisions, judicial pronouncements, statutory developments such as the "Digital Personal Data Protection Act, 2023, and relevant international legal frameworks like the General Data Protection Regulation (GDPR) of the European Union".

Various books, research articles, law commission reports, policy documents, official notifications, and legal commentaries have been consulted to understand the theoretical underpinnings and practical dimensions of RTBF. Furthermore, newspaper articles, legal blogs, and online databases such as SCC Online, Manupatra, and the official websites of regulatory authorities have been utilized to gather current and relevant data. The study aims to identify legal gaps, inconsistencies, and evolving judicial trends while comparing the Indian position with global best practices, thereby contributing to the broader discourse on digital privacy and data protection.

IV. OBJECTIVES OF THE STUDY

1. To analyse the legal frameworks and regulatory mechanisms governing the Right to be Forgotten (RTBF) globally, with a focus on understanding their effectiveness in protecting individual privacy rights.

2. To evaluate the moral ramifications of RTBF in striking a balance between freedom of speech and private rights, especially in light of digital memory and online information sharing.

3. To examine the technological challenges associated with implementing RTBF, including data deletion, storage, and cross-border data transfers, and propose solutions to enhance compliance and effectiveness.

4. To investigate the societal and cultural factors influencing the interpretation and application of RTBF laws across different jurisdictions, aiming to identify best practices and lessons for global implementation.

5. To provide recommendations for policymakers, legal professionals, and stakeholders on enhancing RTBF legislation and enforcement mechanisms to better protect individual privacy rights in the digital age.

V. HYPOTHESIS

1. The implementation of the Right to be Forgotten (RTBF) in India will face significant challenges due to the lack of specific legal provisions addressing its nuances, leading to ambiguity and inconsistency in its application.

2. The Right to be Forgotten will not be practically applicable in India due to ambiguities in the present legal framework and unclear enforcement procedures, which would lead to uneven results for anyone attempting to exercise this right.

VI. SIGNIFICANCE OF THE STUDY

The present study on the "Laws Relating to Right to be Forgotten in India: Issues and Challenges" holds considerable significance in the contemporary digital age, where the intersection of technology, privacy, individual rights, and legal frameworks has become increasingly complex and consequential. In a country like India, where internet penetration has grown exponentially and the digital ecosystem encompasses various spheres of personal and professional life, the issue of data privacy and the right to control one's digital identity has emerged as a pressing concern. The study is timely and relevant, particularly in light of the expanding discourse around the Right to be Forgotten (RTBF) and its place within the broader legal and constitutional framework of India, with the following particular significance as specified below:

1. The study's significance lies in its contribution to legal discourse, particularly in the Indian context. Thoroughly analysing the legal framework surrounding the Right to be Forgotten (RTBF) offers valuable insights to policymakers, legislators, and legal practitioners. Identifying gaps and ambiguities in existing laws, the study informs the development of RTBF policies and regulations, guiding policymakers in striking a balance between privacy rights and freedom of expression.

2. Moreover, the study addresses ethical considerations inherent in RTBF implementation. Exploring complex ethical dilemmas such as privacy, censorship, and historical accuracy fosters informed ethical decision-making. This is crucial in navigating the nuanced landscape of privacy rights and digital governance, ensuring that RTBF mechanisms uphold ethical principles while protecting individual autonomy.

3. Practical challenges hindering the effective implementation of RTBF in India are also a focus of the study. By evaluating issues related to technological feasibility, intermediary liability, and enforcement mechanisms, the study proposes pragmatic solutions to enhance the efficiency and effectiveness of RTBF mechanisms. Addressing these challenges is essential for the successful implementation of RTBF and the protection of individual privacy rights in the digital age.

4. Additionally, the survey clarifies how Indian society views and feels about RTBF. It fosters a deeper understanding of the importance of data protection, digital governance, and privacy rights by raising awareness among citizens, IT professionals, legislators, and civil society. To promote informed public debate and create policies that reflect the needs and values of Indian society, social awareness is essential.

VII. REVIEW OF LITERATURE

A- Books

1. "Data Privacy and GDPR Handbook"[22]

• "Data Privacy and GDPR Handbook" by Sanjay Sharma is a comprehensive guide that provides organizations with essential knowledge and practical tools to navigate and comply with data privacy laws, particularly the General Data Protection Regulation (GDPR). This book addresses the critical need for stringent data privacy measures and offers solutions that facilitate compliance, making it an invaluable resource for data officers and compliance managers.

• One of the key findings of Sharma's work is the comprehensive framework it offers for GDPR compliance. The book delves into the history and foundation of data privacy laws, providing a detailed roadmap for organizations to achieve and maintain compliance. Additionally, the book includes practical strategies for setting up GDPR compliance departments, offering step-by-step guidance that is particularly useful for businesses navigating these complex regulations for the first time. Case studies and real-world examples of GDPR enforcement are also featured, illustrating the challenges companies face and the solutions they implement to adhere to data privacy regulations.

However, despite its extensive coverage of GDPR and global data privacy implications, the book does not specifically address the challenges and issues related to implementing the Right to be Forgotten in India. This represents a notable gap in the literature, as the adaptation and enforcement of such privacy rights within the Indian legal framework require careful consideration and tailored solutions. Further research could explore this area, examining how India's unique socio-legal landscape influences the practical application of RTBF and identifying potential pathways for legislative and regulatory development.

2. "Data Protection Law and Practice"[23]

• "Data Protection Law and Practice" by Rosemary Jay is a comprehensive legal reference that covers the intricacies of data protection laws. The book is renowned for its in-depth analysis of data privacy regulations and their practical implications, making it a vital resource for legal professionals and scholars in the field of data protection. The relevance of this book to the topic "Laws Relating to Right to be Forgotten in India: Issues and Challenges" is significant. Jay's detailed exploration of GDPR provides insights into the implementation and challenges of data protection laws, which are pertinent to understanding the RTBF. By comparing GDPR with emerging data privacy laws in India, readers can gain a comprehensive understanding of the issues and challenges specific to the Indian context.

While the book extensively covers GDPR, it does not specifically address the challenges and issues related to implementing the Right to be Forgotten in India. This gap underscores the need for further research on how RTBF can be effectively integrated into India's legal framework, given the country's unique socio-legal landscape.

[22]*Sanjay Sharma, Data Privacy and GDPR Handbook (Wiley publications, 2nd Edition, 2019).*
[23]*Rosemary Jay, Data Protection Law and Practice (Sweet & Maxwell pb., 1stedn., 2018).*

3. "Information Technology Law and Practice"[24]

• "Information Technology Law and Practice" by Vakul Sharma is a comprehensive book that delves into the various aspects of IT law in India. This book offers a comprehensive examination of the legal framework governing information technology, including the legislative and regulatory measures implemented to address issues arising from the use of technology in various sectors. It covers topics such as cybercrime, electronic commerce, data protection, and intellectual property rights in the context of information technology.

• Key findings from the book include a comprehensive overview of the Indian IT Act, its amendments, and the rules framed under it, which are crucial for understanding the legal framework for data protection in India. Sharma discusses the challenges in implementing these laws, including enforcement issues and the need for a more robust regulatory framework to deal with emerging technologies and cyber threats. The book also examines international perspectives on data protection and compares them with Indian laws, providing a broader context for understanding the global nature of data privacy issues.

One of the key gaps in the literature identified by this book is the lack of specific provisions related to the RTBF within the Indian legal framework. While the book extensively covers data protection and privacy laws, it highlights the need for more comprehensive legislation that specifically addresses the RTBF. This gap suggests a significant area for further research and development in Indian law to adequately protect individuals' rights in the digital age.The book "Information Technology Law and Practice" by Vakul Sharma thus serves as an essential resource for understanding the current state of IT law in India, its relevance to data protection and the RTBF, and the areas where further legal developments are necessary.

4. Delete The Virtue of Forgetting in the Digital Age [25]

• In "Delete: The Virtue of Forgetting in the Digital Age," Viktor Mayer-Schönberger delves into the critical issue of how digital technology's capacity to store vast amounts of information indefinitely poses significant challenges to privacy, personal development, and societal functioning. He argues that forgetting is an essential human function that helps individuals and societies evolve and progress. By highlighting the importance of temporary information, Mayer-Schönberger advocates for implementing mechanisms that introduce "digital forgetting" into our data management practices. He presents a comprehensive analysis of the psychological, social, and legal ramifications of perpetual data storage and proposes potential solutions to balance the benefits of data retention with the necessity of forgetting.

However, there is a notable gap in the literature regarding the application of these concepts to the Indian legal and cultural context. While Mayer-Schönberger provides a strong theoretical framework, there is a need for more specific research that addresses how RTBF can be effectively implemented and enforced in India. This involves considering India's unique legal challenges, societal norms, and the technological landscape. Further studies are necessary to explore how India can adapt and apply RTBF principles within its jurisdiction to protect its citizens' privacy in the digital age.

5. "Unlocking Our Data-Driven Future"[26]

• Rahul Matthan's Privacy 3.0 is a policy-forward and practitioner-oriented book that situates India's privacy conversation within the broader global shift toward a

[24]*Vakul Sharma, Information Technology Law and Practice(Universal Law Publishing, 1stedn., 2020).*
[25]*Viktor Mayer-Schönberger, delete: The Virtue of Forgetting in the Digital Age(Princeton University Press, 1stedn., 2011).*
[26]*Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins, India, 1st edn., 2021).*

data-driven economy. Matthan traces the evolution of privacy norms and demonstrates how technological change — including big data, AI, and digital public infrastructures -necessitates new regulatory thinking that extends beyond simple prohibition or heavy-handed secrecy. He advocates a pragmatic "third way": rules that protect individuals' dignity and agency while enabling beneficial uses of data.

• The book is particularly useful for students of RTBF because it frames "forgetting" not only as a legal takedown problem but as one part of an ecosystem of data governance tools: minimisation, purpose-limitation, access controls, and redress. Matthan emphasises proportionality, layered accountability, and practical compliance mechanisms for interme diaries and public authorities.

While not a doctrinal legal treatise, the book usefully translates judicial and legislative developments (including the Puttaswamy judgment and India's data-law drafts) into operational guidance which helps situate RTBF within India's emerging data protection architecture. The tone is pragmatic: protect privacy, enable innovation, and build institutions that can adjudicate competing public and private interests.

6. "Privacy Law: An Indian Perspective"[27]

• Apar Gupta's book blends doctrinal analysis and public-interest advocacy. As a lawyer active in India's digital-rights movement, Gupta maps the constitutional foundations of privacy (especially the Puttaswamy decision) onto concrete regulatory concerns. He analyses privacy not as an isolated right but as one that overlaps with speech, access to information, and democratic governance, a perspective crucial for assessing RTBF. Gupta is careful about the risks of overbroad delisting and the potential for powerful actors to weaponize removal requests.

• His chapters evaluate international models (EU GDPR, U.S. approaches) and emphasize context-sensitive balancing tests and transparent procedural safeguards if RTBF mechanisms are to be adopted in India.

For scholars, the book's strength is its attention to civil-society perspectives, policy trade-offs, and the need for accountability mechanisms (independent oversight, right of appeal, public interest exceptions) in any RTBF regime. Gupta argues that India must design remedies that protect individuals without undermining press freedom or the historical record.

B- Research Papers & Scholarly Articles

7. Right to Be Forgotten in India: A Critical Legal Analysis[28]

• "Right to Be Forgotten in India: A Critical Legal Analysis" by A. Rajat and G. Bharti provides an in-depth examination of the RTBF within the Indian legal context. The paper, published in the Indian Journal of Law & Legal Research in 2022, critically analyses the evolution, challenges, and application of the RTBF in India. It examines the legal framework surrounding data privacy in India, particularly in light of global developments such as the GDPR, and evaluates how the Indian legal system has addressed the need for a similar right.

8. The Need for the Right to Be Forgotten in India[29]

• "The Need for the Right to Be Forgotten in India" by Tejashree J. explores the necessity and implications of establishing the Right to Be Forgotten (RTBF) within the

[27] *Apar Gupta, Privacy Law: An Indian Perspective (LexisNexis/Academic Press, 1stedn., 2019).*
[28] *Rajat, Anuprash, Gaurav Bharti, et.al., "Right to Be Forgotten in India: A Critical Legal Analysis" 1(4) Indian JL & Legal Rsch (2022).*
[29] *J. Tejashree, "The Need for the Right to Be Forgotten in India" 5 RGNUL Financial and Mercantile Law Review106 (2018).*

Indian legal framework. Published in the RGNUL Financial and Mercantile Law Review in 2018, the article highlights the increasing significance of data privacy in the digital era and advocates for the recognition of RTBF as a fundamental right in India.

However, the literature gap identified pertains to the practical enforcement of RTBF in India. While the article provides a thorough theoretical analysis, further research is needed to explore the logistical and regulatory challenges of implementing RTBF in a diverse and populous country like India.

9. Right to Be Forgotten: A Critical and Comparative Scrutiny between India and the European Union[30]

• The right to be forgotten addresses a common concern: the lasting impact of personal information posted online. In the digital realm, content remains accessible even years after its initial publication. Individuals seek autonomy by requesting the removal of private information from internet searches. This controversial right has sparked global discussions, with some countries adopting and implementing it, while others remain dissenting.

• The right to be forgotten aligns with fundamental principles of human dignity. It recognizes that individuals should have control over their digital legacy, especially when past actions no longer reflect their present circumstances.

While the paper provides valuable insights, it identifies a gap in existing literature: empirical studies specifically analysing the impact of the right to be forgotten in India and the EU are limited. Further research is needed to explore user experiences, legal compliance, and the effectiveness of mechanisms for data removal.

10. Right To Be Forgotten in India: Exploring the Uncharted Territory[31]

• The paper delves into the challenge of preserving privacy and maintaining anonymity in the digital era. It emphasizes the difficulty individuals face in achieving true anonymity, given the pervasive influence of social media and search engines. The concept of the "right to be forgotten" aims to empower individuals to remove their data from online platforms, subject to specific conditions.

Within this uncharted territory, the paper identifies a crucial gap related to the removal of court judgments from official records. While the right to be forgotten has gained prominence, practical implications and limitations remain largely unexplored in the Indian context. Further research is essential to navigate these complexities effectively.

11. Reconciling Personal Information in the United States and European Union[32]

• Schwartz, Paul M., and Solove, Daniel J., "Reconciling Personal Information in the United States and European Union," 102 California Law Review 877 (2014), offers an insightful comparison of data privacy laws between the United States and the European Union. The article explores the fundamental differences in how personal information is treated across these jurisdictions, with the EU adopting a more comprehensive regulatory approach through instruments like the GDPR, which includes provisions such as the Right to Be Forgotten. The authors analyse the cultural and legal underpinnings that drive these differences and propose ways to bridge the gap between the two systems.

The literature gap identified in the article pertains to the

[30]*Rohith K., "Right to Be Forgotten: A Critical and Comparative Scrutiny between India and European Union" 4(1)Indian Journal of Law and Legal Research1 (2022).*
[31]*Malhotra, Sehaj, and Shreya Saxena. "RIGHT TO BE FORGOTTEN IN INDIA: Exploring the Uncharted Territory" 10(5)SSRN Electronic Journal109(2024).*
[32]*Paul M. Schwartz, and Daniel J. Solove, "Reconciling Personal Information in the United States and European Union" 102California Law Review877-919 (2014).*

need for more empirical studies that assess the impact of these differing privacy laws on individuals and businesses. Specifically, there is a call for research that explores how the principles outlined can be effectively applied in diverse legal landscapes, such as India, where socio-economic and cultural factors significantly influence the shaping of privacy norms.

C-Government Committee Reports:

12. Justice B. N. Srikrishna (Committee) White Paper / Report on Data Protection: A Free and Fair Digital Economy (Justice B.N. Srikrishna Committee, 2018):

• Though a committee report rather than a conventional monograph, the Srikrishna Committee's white paper is foundational for India's data protection debate. Chaired by retired Justice B. N. Srikrishna, the report proposed a comprehensive framework that later influenced legislative drafts. For RTBF, the Committee explicitly recognized the need for data-subject rights that include correction and erasure in specific circumstances and recommended a proportional, rights-based framework with exceptions for free expression, archival needs, and public interest.

• The report's analytical strength lies in reconciling individual autonomy with legitimate collective uses of data; it flags the operational challenges, such as jurisdictional limits, global intermediaries, and archival retention, that any RTBF mechanism must solve. Scholars rely on this document for primary policy language and for understanding the balancing approach Indian policymakers initially favored.

Its recommendations shaped subsequent bills and remain a key reference point when critiquing the DPDP Act's approach to erasure and delisting.

13. Ministry of Electronics and Information Technology, "The Personal Data Protection Bill, 2019 – Explanatory Note"[33]

• This explanatory note accompanied the introduction of the Personal Data Protection Bill in Parliament, offering insights into the statutory grounding of RTBF in India. It clarified that RTBF would empower data principals to prevent disclosure of personal information if it served no legitimate purpose, had become irrelevant over time, or was excessively intrusive. The note also outlined exceptions, such as the right to retain data for legal compliance, journalistic purposes, or public interest. The Bill's Clause 20 directly referenced RTBF, linking it to informational privacy as recognised in K.S. Puttaswamy v. Union of India. The explanatory document further highlighted that RTBF enforcement would require a quasi-judicial authority to ensure proportionality and necessity, preventing arbitrary censorship.

This note has become a key interpretative aid for legal scholars analyzing RTBF's legislative intent in India, although the Bill has since undergone changes and been replaced by the Digital Personal Data Protection Act, 2023, which omits an explicit RTBF provision.

CONCLUSION AND SUGGESTIONS

The study establishes that the Right to Be Forgotten (RTBF) has become a crucial element of modern privacy law, particularly in an era where digital information persists indefinitely and can affect individuals long after it ceases to hold public relevance. While the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India provides the constitutional basis for RTBF, the absence of a specific statutory provision results in fragmented judicial approaches and uncertainty in enforcement. The

[33]*Ministry of Electronics and Information Technology, "The Personal Data Protection Bill, 2019 – Explanatory Note" (Government of India, 2019).*

Digital Personal Data Protection Act, 2023, offers a limited erasure mechanism but does not expressly incorporate RTBF, leaving key issues unresolved, including intermediary obligations, standards for delisting, and safeguards against misuse. The analysis underscores the necessity for a comprehensive, balanced, and rights-based legal framework that safeguards personal autonomy without compromising freedom of expression, public access to information, and institutional transparency.To address these concerns, the study recommends the explicit incorporation of RTBF into India's data protection laws through clear legislative provisions defining its scope, grounds, and exceptions. A specialised adjudicating authority should evaluate RTBF claims based on proportionality and public interest. Intermediaries should be assigned well-defined compliance responsibilities to ensure predictable and transparent delisting procedures. Technical protocols for effective data removal and suppression must be developed to overcome challenges posed by digital permanence. Judicial guidelines should be standardised to promote consistency across decisions. Strengthening public awareness and institutional capacity is essential for effective implementation. Integrating RTBF with broader data governance principles, such as data minimization, purpose limitation, and accountability, will ensure a balanced and robust protection of privacy in the digital age.

GUARDIANS OF DATA: FROM BRUSSELS TO BHARAT

Anaji Aggarwal*

Dr Rahul Varshney**

I. INTRODUCTION

In the rapidly evolving digital era, the concept of privacy has undergone a significant transformation. Historically, privacy was perceived primarily as a personal boundary, a sphere of autonomy in which individuals could exercise control over their personal lives without interference from external entities.[1] However, the proliferation of the internet, social media platforms, and smart technologies has fundamentally altered the dynamics of privacy. Today, personal information is continuously collected, monitored, and analyzed by both private corporations and government agencies. The pervasive nature of this digital environment raises pressing questions regarding the protection of individual freedoms and the balance between technological innovation and personal autonomy (Solove, 2021).The right to privacy has long been recognized as a cornerstone of democratic societies. In the Indian context, privacy was historically considered an implicit aspect of the fundamental right to life and personal liberty under Article 21 of the Constitution of India[2]. This understanding evolved over time, influenced by judicial interpretations and the growing complexities of a digitized society. The landmark judgment of Justice K.S. Puttaswamy v. Union of India (2017) explicitly recognized privacy as a constitutionally protected fundamental right, affirming its centrality to human dignity and autonomy[3]. The judgment marked a watershed moment in Indian jurisprudence, highlighting the need to reconcile individual rights with the demands of state surveillance, national security, and the expanding digital economy. The advent of large-scale data collection, artificial intelligence (AI), and predictive analytics has introduced new challenges to the traditional understanding of privacy. Digital platforms routinely gather vast quantities of personal information for commercial purposes, such as targeted advertising, behavior tracking, and user profiling. Simultaneously, governments utilize digital surveillance for law enforcement, taxation, and national security objectives. These practices raise complex ethical and legal concerns regarding consent, data ownership, and potential misuse of sensitive information (Zuboff, 2019). For instance, the lack of transparency in data processing can erode trust between individuals and digital service providers, compromising the fundamental principles of democracy and human dignity[4]. Digital rights, encompassing the protection of privacy, freedom of expression, and access to

*Research Scholar MVN University Palwal Haryana
**Dean, Law Depatment, MVN University Palwal Haryana
[1]Privacy, in classical legal theory, is often defined as the right of an individual to seclude themselves and control personal information.
[2]Article 21 of the Constitution of India guarantees the right to life and personal liberty, which courts have interpreted to include privacy.
[3]K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[4]Zuboff, S. (2019) highlights the ethical challenges posed by surveillance capitalism in which personal data is monetized without sufficient consent.

information, have thus become increasingly central to discussions on human rights in the twenty-first century. Scholars emphasize that legal compliance alone is insufficient; ethical governance, transparency, and citizen empowerment are equally essential to safeguard digital freedoms (Westin, 1967; Solove, 2008). In the Indian context, this entails not only robust legislative measures, such as the proposed Personal Data Protection Bill, 2019, but also public awareness initiatives and digital literacy programs that enable individuals to navigate the complex digital landscape safely and responsibly[5]. This research paper aims to explore the evolving nature of digital rights, focusing on the right to privacy in the information age, particularly in India. It seeks to answer critical questions regarding the legal, ethical, and social dimensions of digital privacy: How has the concept of privacy evolved in response to technological advancements? What challenges arise from government surveillance and corporate data practices? How can legal frameworks be strengthened to ensure the protection of individual freedoms? Through a comprehensive analysis of judicial pronouncements, statutory provisions, and international best practices, this paper intends to provide insights into the ways in which digital privacy can be effectively safeguarded while promoting technological innovation and societal development. The study underscores the necessity of recognizing privacy as a core component of digital rights and advocates for updated legal interpretations and enforcement mechanisms that reflect the realities of the digital age. By situating the Indian experience within a comparative international framework, the research highlights both the opportunities and challenges associated with protecting digital freedoms in a globalized world. Ultimately, the paper argues that the protection of privacy is not merely a legal obligation but a fundamental ethical imperative, central to the preservation of human dignity, autonomy, and trust in the digital era.

2. Evolution of the Right to Privacy in India

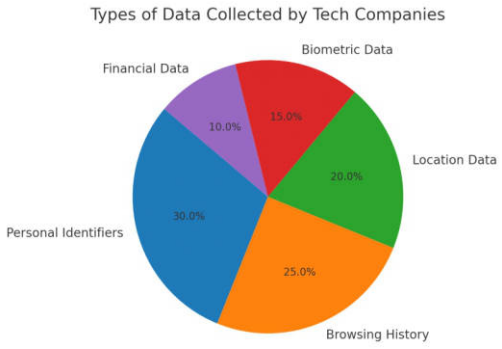
The concept of privacy in India has evolved significantly over time, shaped by both judicial interpretation and societal changes. Prior to the recognition of privacy as a fundamental right, Indian law approached it implicitly through various provisions of the Constitution and common law doctrines. Traditionally, privacy concerns were addressed under the umbrella of personal liberty and the right to life as guaranteed by Article 21 of the Constitution of India[6]. Courts historically recognized limited aspects of privacy, such as the confidentiality of correspondence, protection from unlawful searches, and individual autonomy in personal matters. Early landmark cases laid the groundwork for privacy jurisprudence in India. In M.P. Sharma v. Satish Chandra (1954), the Supreme Court addressed the issue of search and seizure in the context of constitutional protection, highlighting the need to safeguard personal liberty against arbitrary state action[7]. Subsequently, in Kharak Singh v. State of Uttar Pradesh (1962), the Court examined police surveillance practices, ruling that domiciliary visits and monitoring of movements violated the reasonable expectation of privacy[8]. Although these cases recognized aspects of privacy, they did not explicitly declare it as a fundamental right.

[5]Digital literacy initiatives play a crucial role in enabling citizens to exercise their rights responsibly in the digital space.
[6]Article 21 of the Constitution of India guarantees the right to life and personal liberty, which has been interpreted to include privacy.
[7]M.P. Sharma v. Satish Chandra, AIR 1954 SC 300; addressed constitutional safeguards against search and seizure.
[8]Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295; recognized limits on state surveillance.

The turning point in the legal understanding of privacy came with the 2017 landmark judgment of Justice K.S. Puttaswamy v. Union of India. In this case, a nine-judge bench of the Supreme Court unanimously held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21 and is therefore a fundamental right[9]. The Court emphasized that privacy encompasses personal autonomy, informational privacy, decisional autonomy, and bodily integrity. The judgment also clarified that privacy is not absolute; it may be restricted by law for reasons such as national security, public order, or the protection of the rights of others, but such restrictions must satisfy the tests of legality, necessity, and proportionality[10].

Following the Puttaswamy judgment, the legal discourse on privacy expanded to include digital dimensions. The proliferation of the internet, mobile technologies, and social media platforms introduced new challenges, necessitating legal interpretations that could address digital surveillance, data collection, and profiling. The case of Justice K.S. Puttaswamy recognized that privacy extends to digital spaces, establishing a foundation for the regulation of personal data and online autonomy. In India, digital privacy is now increasingly viewed not just as a personal concern but as a legal right requiring protection from both governmental overreach and corporate exploitation. Comparatively, international frameworks offer valuable insights into the evolution of privacy rights. The European Union's General Data Protection Regulation (GDPR) establishes stringent rules on data collection, consent, and individual rights over personal information[11]. In the United States, privacy is protected through sector-specific legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA), alongside judicial recognition of privacy in constitutional law. By examining these international models, India can adopt best practices to strengthen its own data protection frameworks while respecting constitutional principles[12]. The evolution of privacy in India illustrates a trajectory from implicit recognition under the broader framework of fundamental rights to explicit constitutional protection in the digital age. The legal framework now acknowledges that privacy is multi-dimensional—covering decisional, bodily, and informational aspects—and that it must adapt continuously to technological innovations. The Puttaswamy judgment serves as both a culmination of historical legal developments and a starting point for future legislative and judicial efforts aimed at safeguarding individual freedoms in an increasingly digital world[13].

3. Challenges to Digital Privacy in the Information Age



[9]*K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; privacy recognized as a fundamental right.*
[10]*Ibid., para. 66; established principles of legality, necessity, and proportionality in restricting privacy.*
[11]*European Union. (2016). General Data Protection Regulation (GDPR); provides comprehensive digital data protection standards.*
[12]*Cate, F. H., & Mayer-Schönberger, V. (2013). Data protection principles. Oxford University Press; comparative study of international privacy frameworks.*
[13]*Solove, D. J. (2021). The digital person: Technology and privacy in the information age. NYU Press; discusses the implications of digital privacy.*

The digital era has fundamentally transformed the landscape of privacy, creating new challenges that traditional legal frameworks were not designed to address. While the recognition of privacy as a fundamental right in India provides a constitutional safeguard, the pervasive use of technology has introduced complexities that make enforcement increasingly difficult. Digital platforms, artificial intelligence, and government surveillance initiatives have created environments in which personal data is continuously generated, collected, and processed, often without full awareness or consent from individuals (Solove, 2021)[14].

One of the most significant challenges to digital privacy is government surveillance. Governments worldwide, including India, deploy digital tools for law enforcement, taxation, national security, and policy planning. In India, initiatives like Aadhaar, the biometric identification system, have raised concerns about the potential for mass surveillance and misuse of personal data[15]. While these programs promise efficiency and transparency, they also pose significant risks to individual autonomy and privacy. The Supreme Court in K.S. Puttaswamy v. Union of India acknowledged that privacy rights are not absolute, but any restriction must adhere to principles of legality, necessity, and proportionality, thereby providing a framework for evaluating government surveillance programs[16]. Corporate data collection presents another major challenge. Social media platforms, e-commerce websites, and digital applications routinely collect user data to facilitate targeted advertising, enhance user experience, and generate revenue. This data often includes sensitive personal information, such as location, health details, and behavioral patterns, which can be analyzed and monetized without explicit consent. The lack of transparency in data handling can lead to unauthorized profiling, discriminatory practices, and even manipulation of public opinion, as observed in global instances such as the Cambridge Analytica scandal (Zuboff, 2019)[17]. Artificial intelligence (AI) and machine learning further complicate digital privacy. AI systems analyze vast datasets to make predictions, automate decisions, and personalize services. While these technologies offer significant benefits, they also risk infringing on privacy rights. For example, predictive policing tools and algorithmic credit scoring can reinforce biases, invade personal autonomy, and create opaque decision-making processes. Individuals often have limited knowledge of how their data is used in AI systems, undermining informed consent and accountability (Cavoukian, 2011)[18]. Consent and data ownership remain critical concerns in the digital age. In many cases, users unknowingly agree to extensive data collection through complex terms and conditions that are difficult to comprehend. This raises questions about the validity of consent, particularly when individuals have limited alternatives to access essential digital services. Moreover, data ownership is often ambiguous, with corporations asserting control over information that pertains to individuals' personal lives, creating an imbalance of power between users and service providers (Solove, 2008)[19].

[14]Solove, D. J. (2021) emphasizes that the rapid pace of technological innovation challenges traditional privacy norms.
[15]Aadhaar is a biometric identification system in India that stores personal information and has raised privacy concerns.
[16]K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; highlighted the principles of legality, necessity, and proportionality.
[17]The Cambridge Analytica scandal involved the misuse of personal data from social media platforms to influence political campaigns.
[18]Cavoukian, A. (2011). Privacy by design: The 7 foundational principles; stresses embedding privacy into technology development.
[19]Solove, D. J. (2008). Understanding privacy; discusses challenges of consent and data ownership.

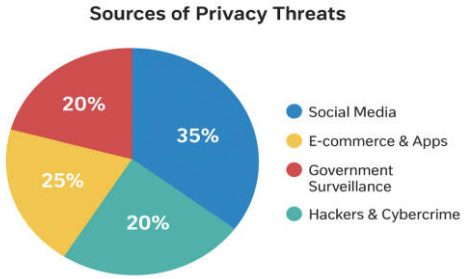
Another pressing challenge is the ethical dimension of digital privacy. Beyond legal compliance, ethical governance requires transparency, accountability, and respect for individual autonomy. Surveillance and data collection practices may be technically lawful yet morally questionable if they exploit vulnerabilities or manipulate behavior. For example, targeted advertising based on sensitive health or political data may not violate existing laws but can significantly impact personal freedoms and democratic processes (Zuboff, 2019)[20].

Furthermore, the global nature of digital networks complicates regulatory oversight. Data often crosses national boundaries, raising jurisdictional issues and complicating enforcement of privacy protections. International frameworks like the European Union's GDPR set standards for data protection, but countries such as India are still in the process of aligning domestic laws with global best practices. Without effective cross-border cooperation and comprehensive legal frameworks, individuals' privacy remains vulnerable to exploitation in the digital ecosystem (Cate & Mayer-Schönberger, 2013)[21]. In conclusion, the challenges to digital privacy in the information age are multi-dimensional, involving technological, legal, ethical, and social aspects. Government surveillance, corporate data practices, AI, and consent complexities all contribute to an environment where personal information is continuously at risk. Addressing these challenges requires a combination of robust legal frameworks, ethical governance, digital literacy, and international cooperation. The recognition of privacy as a fundamental right in India provides a constitutional foundation, but effective protection in practice necessitates proactive measures to safeguard personal autonomy, transparency, and trust in the digital environment[22].

4. Legal and Policy Frameworks for Protecting Privacy

The recognition of privacy as a fundamental right in India through the Puttaswamy judgment of 2017 provided the constitutional foundation for privacy protection, yet the practical enforcement of this right depends largely on robust legal and policy frameworks. In the information age, where data is constantly collected, shared, and monetized, the challenge lies not only in recognizing privacy as a right but also in implementing effective mechanisms to safeguard it. This section critically examines the Indian legal framework, the status of the Personal Data Protection Bill, international conventions, and the enforcement challenges that persist.

Indian Legal Framework



India's first formal attempt to regulate data protection came through the Information Technology Act, 2000 (IT Act), particularly Sections 43A and 72A[23]. Section 43A mandates that companies handling sensitive personal data must implement "reasonable security practices" to protect it from misuse, while Section 72A criminalizes unauthorized disclosure of information. While these

[20]*SZuboff, S. (2019). The age of surveillance capitalism; explores ethical concerns in digital data exploitation.*
[21]*Cate, F. H., & Mayer-Schönberger, V. (2013). Data protection principles; compares international frameworks for privacy protection.*
[22]*Effective privacy protection requires integrating legal, ethical, and technological safeguards.*
[23]*Information Technology Act, 2000, Sections 43A and 72A.*

provisions represent a step forward, they are narrow in scope and lack comprehensive safeguards for personal data in the digital ecosystem. The Justice K.S. Puttaswamy v. Union of India judgment emphasized the need for a robust legislative framework to give substantive effect to the right to privacy. In response, the government introduced the Personal Data Protection Bill (PDP Bill), 2019. Inspired by the European Union's General Data Protection Regulation (GDPR), the Bill sought to regulate the collection, storage, and processing of personal data by both state and private entities. It introduced principles such as informed consent, data minimization, purpose limitation, and the establishment of a Data Protection Authority (DPA) to oversee compliance. However, the Bill has been subject to criticism. Scholars argue that its broad exemptions for government agencies undermine the very foundation of privacy as a fundamental right (Basu, 2020).^5 For instance, the Bill allows the central government to exempt any agency from its provisions on grounds of national security, public order, or friendly relations with foreign states. Critics contend that such vague exemptions risk legitimizing surveillance practices without adequate checks and balances. Furthermore, the withdrawal of the PDP Bill in 2022 and its replacement with the Digital Personal Data Protection Act, 2023, highlights ongoing tensions between privacy protection and state interests. The new Act, while streamlining certain provisions, has also been critiqued for granting wide powers to the government over data processing exemptions.

International Conventions and Comparative Frameworks

Globally, privacy is recognized as a fundamental human right under international conventions such as Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). These instruments emphasize protection against arbitrary interference with privacy, family, or correspondence. While not directly enforceable, they guide domestic legislation and international cooperation.

The GDPR represents the most comprehensive and influential legal framework for data protection worldwide. It grants individuals rights such as data access, rectification, erasure ("right to be forgotten"), and portability, while imposing strict obligations on data processors. Importantly, it incorporates principles of accountability, privacy by design, and explicit consent. The GDPR's extraterritorial scope ensures that companies outside the EU, including Indian entities offering services to EU citizens, must comply with its provisions. By contrast, the United States adopts a sectoral approach, with privacy regulated through specific statutes such as the Health Insurance Portability and Accountability Act (HIPAA) for health data and the Children's Online Privacy Protection Act (COPPA) for children's data. This fragmented system often leads to uneven protections and reliance on corporate self-regulation. For India, a hybrid model—drawing inspiration from the GDPR's comprehensive rights framework while accommodating sector-specific regulations—may provide a balanced approach.

Enforcement Mechanisms and Challenges

Despite constitutional recognition and legislative efforts, enforcement of privacy rights in India faces several challenges. First, institutional capacity remains

[25] *K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*

limited. Regulatory authorities, such as the proposed Data Protection Board under the 2023 Act, must be equipped with adequate resources, independence, and expertise to effectively oversee compliance. Without genuine autonomy, regulatory bodies risk becoming instruments of state control rather than protectors of individual rights.

Second, the digital ecosystem in India is dominated by powerful corporations that handle massive volumes of data. The asymmetry of power between corporations and individual users makes enforcement of consent-based frameworks particularly difficult. Users often lack meaningful alternatives, and "consent fatigue" caused by lengthy privacy policies undermines the voluntariness of consent (Solove, 2008)[25].

Third, cross-border data flows present jurisdictional challenges. In the absence of strong international cooperation, enforcement of privacy laws across borders remains difficult. Data localization provisions, such as those debated in the PDP Bill, highlight the tension between protecting national sovereignty and facilitating global digital trade.

Lastly, the lack of widespread digital literacy exacerbates enforcement difficulties. Many individuals are unaware of their rights or unable to exercise them effectively. Strengthening legal protections must therefore go hand-in-hand with raising public awareness and building technological literacy among citizens.

India's journey towards building an effective legal framework for privacy reflects the complexities of balancing individual freedoms with state and corporate interests. While constitutional recognition provides a strong foundation, the real challenge lies in creating transparent, enforceable, and citizen-centric laws. Lessons from international frameworks, particularly the GDPR, highlight the importance of accountability, explicit consent, and strong enforcement mechanisms. For India, the way forward must combine robust legal protections with institutional independence, digital literacy, and international collaboration to ensure that privacy in the information age is not merely a theoretical right but a practical reality.

5. Reassessing Privacy as a Digital Right

5.1 Privacy as an Enabler of Other Rights

The right to privacy does not exist in isolation; it is a foundational right that enables the exercise of several other constitutional and human rights. In the Justice K.S. Puttaswamy v. Union of India (2017) case, the Supreme Court of India recognized privacy as intrinsic to life and personal liberty under Article 21 of the Indian Constitution. Without privacy, individuals cannot meaningfully exercise rights such as freedom of speech, freedom of association, or the right to identity.

For instance, surveillance and data tracking can create a chilling effect on free speech, discouraging individuals from expressing dissenting or unpopular opinions. Similarly, the freedom of association is undermined when governments or corporations monitor social groups, online activities, or protest participation. The right to identity, including control over personal information and sexual orientation, is also intrinsically linked to privacy. Landmark judgments such as Navtej Singh Johar v. Union of India (2018), which decriminalized homosexuality, relied heavily on the constitutional guarantee of privacy and dignity.

Thus, privacy serves as an enabling right that fortifies

[25]*Solove, D. J. (2008). Understanding privacy; discusses consent fatigue and power imbalances in privacy regimes.*

the broader framework of democracy and ensures individuals can exercise their freedoms without coercion or fear.

5.2 Ethical Governance vs. Mere Compliance

In the digital age, privacy protection has often been reduced to compliance with regulatory frameworks. For example, companies frequently adopt privacy policies to meet the requirements of data protection laws, such as the Digital Personal Data Protection Act, 2023 in India or the EU General Data Protection Regulation (GDPR). However, compliance alone is insufficient to safeguard dignity and freedom.

The distinction between ethical governance and compliance lies in intent and execution. Compliance is minimalistic—organizations adhere to the letter of the law while often exploiting legal loopholes. Ethical governance, in contrast, recognizes privacy as a moral and democratic value. Companies such as Apple have attempted to integrate privacy into product design ("privacy by default"), while others continue to monetize user data aggressively under the guise of consent.

As scholars argue, true privacy protection requires a rights-based approach rather than a market-based model.[26] A compliance-driven system risks becoming a "tick-box exercise," while ethical governance emphasizes accountability, transparency, and fairness in handling user data.

5.3 Importance of Digital Literacy

Legal safeguards cannot be effective unless individuals understand their digital rights. Digital literacy empowers citizens to make informed choices about data sharing, recognize risks, and demand accountability from both states and corporations.

In India, digital illiteracy remains a major obstacle. With the rapid expansion of initiatives like Digital India and Aadhaar-linked services, millions of individuals—especially in rural areas—have been compelled to share biometric and personal information without fully understanding the implications.[8] This creates asymmetry: corporations and governments wield immense technological power, while individuals remain vulnerable.

Comparatively, countries in the European Union have invested heavily in public awareness campaigns following the implementation of GDPR, ensuring that individuals understand their rights to data portability, erasure, and rectification[27]. For India, similar initiatives are urgently required, especially in vernacular languages, to bridge the gap.

Digital literacy must also include awareness of cyber hygiene—recognizing phishing, protecting passwords, using encryption, and managing digital footprints[28]. Without this, even the strongest data protection laws cannot shield citizens from exploitation.

5.4 Privacy in the Context of Democracy and Human Dignity

At its core, the right to privacy is not merely about data—it is about human dignity and democracy. Democracy thrives on free participation, dissent, and plurality of voices. Constant surveillance, whether by the state or corporations, erodes these freedoms by creating fear and conformity[29]. The Supreme Court of India, in Justice Puttaswamy (2017), explicitly tied

[26]*Westin, A. F. (1967). Privacy and freedom. Atheneum.*
[27]*Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. Communications, 39(3), 283–303.*
[28]*Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.*
[29]*Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs.*

privacy to dignity, declaring that "privacy is the constitutional core of human dignity." Internationally, Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) enshrine privacy as essential for the protection of human dignity. Moreover, digital privacy strengthens democracy by ensuring equality. Data profiling often leads to discrimination, such as algorithmic bias in hiring, policing, or credit scoring. Protecting privacy ensures individuals are not reduced to data points but are treated with fairness and respect. Thus, the recognition of privacy as a digital right is not just a matter of compliance or regulation—it is a reaffirmation of constitutional values and democratic ethics.

6. Recommendations and Future Prospects

6.1 Stricter Enforcement Mechanisms

While India has enacted the Digital Personal Data Protection Act, 2023 (DPDPA), enforcement remains a key challenge. The Act introduces obligations on data fiduciaries, principles of lawful processing, and penalties for violations. However, its enforcement architecture is still evolving. The establishment of the Data Protection Board of India is a step forward, but critics argue that independence and resources are crucial to prevent the board from becoming another bureaucratic authority.

The European Union's General Data Protection Regulation (GDPR) offers a useful precedent. Under GDPR, data protection authorities across member states have issued record fines—such as the €1.2 billion fine against Meta in 2023 for transferring EU data to the U.S. India's enforcement regime must similarly empower regulators to impose proportionate penalties, mandate audits, and ensure accountability of both public and private actors.

6.2 Cross-Border Data Regulation

In an interconnected digital economy, data rarely remains within national boundaries. Cross-border data flow raises concerns about jurisdiction, accountability, and protection. The DPDPA 2023 allows the government to restrict transfer of personal data to certain countries. However, unlike the GDPR, which requires adequacy decisions before permitting transfer, India's approach remains discretionary.

Judicial precedents also emphasize the importance of sovereignty and individual rights in cross-border data issues. In Google v. CNIL (2019), the Court of Justice of the European Union held that the "right to be forgotten" under GDPR does not extend globally, balancing privacy against territorial limits. India must adopt a clear framework for cross-border data regulation, with bilateral and multilateral agreements, while ensuring user rights are not compromised.

6.3 Role of Judiciary, Legislature, and Civil Society

The judiciary has been instrumental in shaping privacy jurisprudence. The Puttaswamy (2017) judgment not only recognized privacy as a fundamental right but also underscored its role in dignity and liberty. Subsequent cases, including Internet and Mobile Association of India v. Reserve Bank of India (2020), where the Supreme Court struck down the RBI's cryptocurrency ban, reflected the balancing of innovation and

[30]*Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*
[31]*Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (1948); International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.9*
[32]*Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104, 671–732.*
[33]*Court of Justice of the European Union (CJEU), Meta Platforms Ireland Ltd v. Data Protection Commission, Case C-252/21 (2023).*
[34]*Google v. Commission nationale de l'informatique et des libertés (CNIL), C-507/17, EU:C:2019:772.*

individual freedoms[35].

The legislature must ensure constant updating of digital rights laws to address emerging technologies like AI and blockchain. Civil society organizations, such as the Internet Freedom Foundation (IFF), have played a crucial role in creating awareness and pushing back against excessive surveillance measures (e.g., challenges to facial recognition projects in Delhi)[36]. Together, these actors must establish a collaborative ecosystem where digital rights are safeguarded through checks and balances.

6.4 Need for AI Ethics and Responsible Data Innovation

Artificial Intelligence poses unprecedented challenges to privacy. Predictive analytics, facial recognition, and algorithmic profiling risk perpetuating discrimination and eroding autonomy. In India, pilot projects using AI in policing and welfare schemes have already raised concerns of bias and exclusion[37].

Globally, regulatory frameworks are emerging. The EU AI Act (2023) categorizes AI systems into risk levels and prohibits "unacceptable risk" applications like social scoring[38]. India has not yet enacted a comprehensive AI law, but discussions are ongoing under the National Strategy for Artificial Intelligence (NITI Aayog, 2018) and subsequent policy papers[39].

Responsible data innovation requires embedding ethical principles—fairness, accountability, transparency, and human oversight—into AI design and deployment. Failure to adopt such principles risks repeating the mistakes of unchecked data exploitation seen in earlier phases of digital development.

7. Conclusion

Privacy in the information age has moved from being a peripheral concern to becoming the core of human dignity and democracy. The Supreme Court of India, in the landmark Justice K.S. Puttaswamy v. Union of India (2017), recognized the right to privacy as a fundamental right under Article 21, affirming that personal autonomy and dignity are inseparable from democratic values. This recognition has since guided legislative and judicial developments. In recent years, the Digital Personal Data Protection Act, 2023 (India), the General Data Protection Regulation (GDPR, EU, 2018), and China's Personal Information Protection Law (2021) have attempted to address the vulnerabilities created by digital surveillance and data mining. Yet, these frameworks show that mere legal compliance is insufficient without ethical governance. The Cambridge Analytica scandal (2018) and ongoing debates on state surveillance highlight that unchecked technological growth without accountability erodes freedom. Moreover, the digital era requires new interpretations of old rights. Traditional notions of consent and data ownership are inadequate in the face of algorithmic profiling, facial recognition, and artificial intelligence. Courts have begun grappling with this—such as the Delhi High Court's observations in the WhatsApp–Facebook data sharing case (2021), where the balance between corporate interest and user privacy was critically examined. Globally, cases before the European Court of Human Rights on state surveillance (e.g., Big Brother Watch v. UK, 2018) also emphasize that privacy is central to democracy. For

[35]*Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.*
[36]*Internet Freedom Foundation. (2021). Facial Recognition in India: A Threat to Privacy and Civil Liberties.*
[37]*Vidushi Marda & Shivangi Narayan (2020). Data in New Delhi's predictive policing systems. ACM FAT Conference Proceedings.*
[38]*European Parliament and Council. (2023). Artificial Intelligence Act. COM/2021/206 final.*
[39]*NITI Aayog. (2018). National Strategy for Artificial Intelligence: #AIforAll.*

individuals to truly benefit, strong laws must be paired with digital literacy. The Justice B.N. Srikrishna Committee Report (2018) stressed that without citizen awareness, even the best legal safeguards remain ineffective. An empowered digital citizenry, aware of its rights and responsibilities, is as essential as enforcement. Finally, the call to action is clear: Protect Privacy, Protect Freedom. Privacy cannot be seen in isolation—it is the right that enables all others: freedom of speech, association, and identity. Future challenges such as AI ethics, cross-border data governance, and biometric surveillance demand proactive judicial interpretation, responsible legislative action, and active civil society engagement. Thus, the future of digital rights depends not only on laws and precedents but also on embedding ethics and human dignity at the heart of digital governance. Safeguarding privacy is, therefore, synonymous with safeguarding democracy itself.

References

Cases:

- K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
- Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).
- M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).

Statutes and Constitutional Provisions:

- European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- Information Technology Act, 2000 (India).
- Universal Declaration of Human Rights, 1948, Article 12.
- International Covenant on Civil and Political Rights, 1966, Article 17.
- European Parliament and Council. (2023). Artificial Intelligence Act. COM/2021/206 final.

Reports:

- Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.
- NITI Aayog. (2018). National Strategy for Artificial Intelligence: #AIforAll.

Books:

- Cate, F. H., & Mayer-Schönberger, V. (2013). Data protection principles. Oxford University Press.
- Solove, D. J. (2007). The digital person: Technology and privacy in the information age. NYU Press.
- Solove, D. J. (2008). Understanding privacy. Harvard University Press.
- Solove, D. J. (2021). The digital person: Technology and privacy in the information age. NYU Press.
- Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.
- Westin, A. F. (1967). Privacy and freedom. Atheneum.
- Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs.

Journal Articles & Research Papers

- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671–732. https://doi.org/10.2139/ssrn.2477899

- Basu, P. (2020). Revisiting India's data protection framework: A critique of the PDP Bill. Indian Journal of Law and Technology, 16(2), 145–167.
- Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. Privacy Laws & Business International Report, (147), 10–13.
- Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. Communications, 39(3), 283–303.
- Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. Big Data & Society, 1(2). https://doi.org/10.1177/2053951714541861
- Marda, V., & Narayan, S. (2020). Data in New Delhi's predictive policing systems. ACM FAT Conference Proceedings.
- Ramanathan, U. (2018). A decade of biometrics in India: Resistance, persistence, and inevitable acceptance. Indian Journal of Law and Technology, 14(1), 1–20.

Online Sources

- Internet Freedom Foundation. (2021). Facial recognition in India: A threat to privacy and civil liberties. Retrieved from https://internetfreedom.in

THE COMMONS THAT FEED THE MACHINES: POLICY REFLECTIONS ON AI'S USE OF PUBLIC DOMAIN WORKS

K.Ankita Rao[1]
Vishakha Sakharkar[2]

ABSTRACT

The contours of creativity and access to knowledge are being transformed due to the advent in technology, especially Artificial Intelligence (AI). AI relies on large scale data scraping from the online repositories which also include public domain works. While public domain was earlier conceived as a shared cultural resource to enable innovation, the growing practice of using the public domain materials for training of AI, raises a troubling paradox of privatization of what was meant to remain freely accessible. As the AI companies are trying to convert publicly available materials into proprietary datasets and outputs usually under opaque and unregulated circumstances, the digital commons is at a risk of being enclosed under the new technological regime. This paper examines how such an appropriation is carried out through data practices, transforming freely available cultural resources into proprietary algorithmic assets.

The paper carries out a comparative legal and policy analysis of jurisdictions including the United States of America, the European Union, India, Japan etc. in order to study the existing copyright exceptions, database rights and fair use and fair dealing provisions which intersect with the use of the public domain material for AI training. The paper also aims to study how open access and data governance frameworks attempt to preserve the openness of the public domain in the digital ecosystem. Further, the paper evaluates emerging trends surrounding text and data mining and ethical implications of enclosing the digital commons through technological means. The final aim of the study is to raise critical questions and find suitable answers regarding sustainability of public domain as a democratic and accessible space in the age of AI.

Keywords- *Public Domain, Artificial Intelligence, Data Scraping, Digital Commons, Copyright.*

I. INTRODUCTION

Artificial Intelligence (AI) systems, especially which are developed on large language (LLMs) and generative models are heavily reliant on large quantities of data in the form of texts, visuals, audios etc. which comes from the materials in the public domain. While public domain material may be legally free for everyone to use, its role has started to transform because of contemporary AI ecosystem. Public domain material is serving as the raw material for the proprietary models built by large AI firms rather than contributing to the shared cultural commons. This results in creating a layer of proprietary value on the freely accessible public domain and encloses the same.

This paper argues that the AI developers do not necessarily require copyright control over the public domain works. The control that AI firms possess over the model outputs, training data and model

[1]*Assistant Professor (Law), Kalinga University, Raipur*

[2]*Assistant Professor (Law), Kalinga University, Raipur*

architecture are sufficient to enclose the public domain structurally. Scholars have argued that the public domain is fragile is nature which is threatened by not just formal rights expansion but also structural barriers to access and reuse (Boyle, 2008). They have also suggested that platform designs and access gatekeeping practically act as 'law' and have the potential to regulate behaviour. (Lessig, 2004). In the context of AI, while public domain remainsintact even after its use for training AI models, the functional access to it is mediated through platform which monetarily benefit from the same.

This paper examines whether the current legal and policy frameworks are sufficient to protect the access and openness of public domain in the age of AI. The authors have used doctrinal analysis, cross-jurisdictional comparison and theoretical insights to analyze the impact of AI on the enclosure of the cultural commons. The authors have also provided policy and legal recommendations to curb this problem. While they acknowledge that AI companies are not legally wrong in using the public domain materials to train the AI systems, the paper argues that law must respond to the contemporary problem of public domain being over-shadowed by structural and economic displacements.

OBJECTIVES OF THE STUDY

1) To examine whether the use of public domain materials for AI training creates a de-facto enclosure or re-privatization of the commons.

2) To evaluate whether the current copyright and data governance regimes are sufficient to preserve the openness of the public domain.

3) To compare the jurisdictional responses of US, EU, India and Japan for the issues identified.

4) To offer legal and policy recommendations to ensure functional accessibility of the public domain in the age of AI.

PROBLEM STATEMENT

AI companies use huge chunks of public domain material to train their models. While this is legally permissible, it creates a structural problem of access of public domain material by allowing AI companies to exert their proprietary rights over the value-added layer created on top of the public domain material. The law currently lacks mechanisms to ensure transparency, reciprocity and accessibility of the underlying public domain materials.

RESEARCH QUESTIONS

1) Does the use made by AI of the public domain works amount to enclosure of the same?

2) Do copyright and data governance laws adequately preserve the integrity and accessibility of the public domain?

3) What inspirations can be taken from various jurisdictions for better governance of public domain resources in AI training?

4) What policy and legal mechanisms should be adopted in order to ensure meaningful accessibility of public domain materials?

RESEARCH METHODOLOGY

This study is based on a doctrinal and comparative methodology whereby the authors have examined statutory texts, judicial decisions, policy documents and scholarly commentary. The jurisdictions for cross-jurisdictional analysis have been selected based on the diversity of approaches towards the TDM exceptions and public domain governance. The study also places

reliance on theoretical framework based on the theory of enclosure of the cultural commons. The authors have not undertaken any empirical or technical testing. The focus of the study is majorly on normative and legal analysis.

LITERATURE REVIEW

The existing legal scholarship on public domain and intellectual property stresses on the vitality of cultural resources for creativity and innovation.James Boylehas argued that law has started a 'second enclosure movement' by trying to fence freely available material(Boyle, 2008) and such enclosure has a direct negative impact on future creativity. (Lessig, 2004).This enclosure may not necessarily happen because of existing legal regimes, but also as a consequence of the architecture of digital systems which shape user behaviour and have the same effect as a legal provision(Cohen, 2012).Other scholars reveal how private players may have quasi regulatory control through infrastructural dominance. (Zuboff, 2019)(Gillespie, 2018). The legal scholarship on TDM exceptions mainly focus on copyright aspects of it, throwing little or no light on the effect of TDM exceptions on non-copyrighted works.(Caterina Sganga, An EU Copyright Framework for Research , 2025).The scholarship on AI is majorly based on the authorship and originality of AI-generated outputs with no inquiry into how there are structural transformations happening as a consequence of public-domain inputs. (Gervais, 2020)The studies on digital heritage are focused on inequalities in digitization, community rights and representation, however, do not analyze the impact of use of large scale data to train AI systems which ultimately siphons publicly funded cultural material into proprietary outputs.Finally the scholars working on the AI governance and transparency have highlighted the need for accountability in data training but do not speak of use of public domain materials as a form of enclosure of cultural commons (Elkin-Koren, 2020) Therefore, while the existing literature does extensively theorize enclosure, the works lack an analysis on how AI developers are creating a proprietary infrastructural layer on the public domain materials practically enclosing and re-privatizing the same. This study seeks to fill the above-mentioned gap by demonstrating how infrastructural and technical filters convert public-domain works into commercial assets. The study also proposes legal interventions for this structural appropriation of the cultural commons.

CONCEPTUAL UNDERSTANDING OF PUBLIC DOMAIN AND DATA SCRAPING:

In the context of intellectual property rights, the term 'public domain' is described as true commons comprising elements of intellectual property that are ineligible for private ownership. (Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989).)Thus, the contents in public domain can be used by any member of public.There has been much debate about the definition of the public domain and its relationship with copyright law. (G.C. Coggins, 2002). It has not been defined under any international instrument or national laws per se. However, some scholars have made efforts to define it. Ronan Deazley defines the contours of the public domain as a series of categories incorporating- i) works which do not qualify for copyright protection; ii) works which do but are out of copyright term; iii)works where permission to use has

been granted by the copyright owner a priori, and iv) such parts of works which fall on the unprotectable side of the idea-expression line, which are allowed for within the statutory framework.(Deazley R. , 2006). Thus, public domain includes all uses of works that do not require the permission of the copyright owner enabling a more precise and nuanced identification and analysis of its components. (Lindsay, 2018)

The public domain is necessary to maintain a fair copyright balance and maintain access to knowledge as it shows that there is a realm of knowledge that is outside of private control and may be freely used by the public. (Uhlir, 2003). It contains works that may be freely made available and accessible to the public for unrestricted use and exploitation, making it an important source for accessing knowledge. It expands the sphere of knowledge by providing raw materials for the new works to build on. (Uhlir, 2003)

In the recent times, with the advent of AI and use of meta data,the public domain is shrinking resulting in gradual reduction of the collection of creative works that are accessible to the public for unrestricted usage(Sajan, 2022).As large LLMs use the data available in public domain by converting it into a monetizable productthrough systematic input, they promote digitization and value-generation. This results in monetizing the information which freely available to public at large. (Sajan, 2022). While these technologies have made it more convenient to access and distribute creative works, they have also facilitated greater control over the usage of such works through mechanisms like digital rights management (DRM) and other technological measures. Consequently, concerns have been raised regarding the potential for private entities to wield excessive power over the use of creative works, particularly in the context of digital media.

The output of a GenAI model emergesfrom algorithmically mediated statistical associations. Therefore, even a highly detailed prompt only functions as an initial condition for a probabilistic process, not as a direct act of authorial will. The final output is the product of a probabilistic sampling which lacks human intervention(Elmahjub, 2025). AI datasets leverage large databases of scraped information, to which many people contribute, to train their models (Huang S. a., 2023). Further, much of the value comes from the commons, but the profits of the models and their applications may be disproportionately captured by those creating the models, rather than going back into enriching the commons. (Weyl, 2021). Such models use freely available data in the public domain and monetizing the processed information in the name of user friendly and easily accessible data or information. Further, the information which is used as an input in the system is in the form of a proprietary database, the access to which is restricted.

LEGAL AND ETHICAL CHALLENGES

The use of information from the public domain and processing the same for the end user thereby monetizing the processed information is shrinking the public domain. Following are the few challenges that have broaden the above-mentioned challenges:

1. Re-privatisation of public domain: The AI datasets are commercialising the information on the models that are fed the information from the public domain thereby enriching their own self rather than going back into giving it to the commons without any obligation to

further compensate those who contributed to the commons. This process makes a shift from the existing structure of the public domain to making it a partially private domain, the access to which is restricted by the AI companies. This is done by adding layer to be pierced before being able to access the public domain.

2. Database rights and access barriers: Database rights grant the creator of database the power to prevent the extraction or re-utilization of all or a substantial part of its content. AI companies by obtaining such rights are creating the access barrier for the information that was supposed to be freely available in the public domain for everyone's consumption thereby creating a barrier for free access of the information.

3. Transparency and attribution problems: The AI datasets often lack in disclosing the data sources thereby creating the problem of transparency as well as of the attribution. Further, they lack on key aspects of perpetuity of moral rights. Moral rights remain even after the author's death, allowing heirs to demand attribution. Further, there is no protection beyond economic rights. Such rights are not available to the AI databases since it lacks human intervention.

THEORETICAL IMPLICATIONS- THE "DIGITAL ENCLOSURE MOVEMENT"

The concept of 'enclosure' was historically applied to physical commons however, the same has now migrated to the intellectual commons. Many scholars such as James Boyle, have discussed how intellectual commons are enclosed by IPR comparing it to the "Enclosure Movement" in England (Boyle, 2008). Centuries ago, villagers in England used to graze their animals in the open and shared fields (the commons)(Gay, 1905)which were later enclosed by the Parliament through "Enclosure Acts" allowing fencing of these lands by private landlords, converting the commons into private property (Christopher Dyer, 2012). Boyle argues that copyright laws, patent laws, digital rights management etc. are enclosing the common resource of knowledge thereby creating another "Enclosure Movement" fencing the freely sharable information. (Boyle, The Second Enclosure Movement and the Construction of the Public Domain, 2003)

Lawrence Lessig, in his series of works argues that, while traditional enclosure happened through law, the modern enclosure is happening through technology through rules such as codes and architecture embedded in the technology(Lessig, Internet Archive, 2001). He argues that 'regulation by architecture in technology' (such as control over channels or sharing platforms) can control the behaviour of people just like legal rules do. For instance, the fact that a Kindle book cannot be shared even if the use is allowed under the fair use exceptions, controls how people can access a particular piece of work. This places unprecedented power in the hands of private companies who regulate what can be accessed, copied or shared by the people(Lessig, Code and other laws of cyberspace, 1999).

These theories when applied to AI give new insights into these are further enclosing the commons. AI systems are fed on public domain works (which should essentially be publicly accessible) and produce a proprietary model that is built on the informational value of these materials. While the copyright over these is not owned by the AI owners, the enclosure is

infrastructural, controlling a value-added layer on these materials that facilitates access (Lessig, Free Culture, 2004). This is not merely a theoretical claim. Many scholars and policy analysts have observed that such curation and massive digitization favours a few large firms and result in concentration of control over this added layer (Casey, 2020).

This sort of enclosure therefore raises new questions. The traditional copyright regime is not suited to address the questions of privatization of usefulness of the public domain works. The problem is not profit making by these large firms owning the AI systems, but the public's ability to use and benefit from the cultural heritage which is restricted by them (Samuelson, 2024). Further these proprietary interfaces also have limited transparency and reciprocity resulting in a potential to distort the cultural commons(Hacker, 2021).

JURISDICTIONAL ANALYSIS

a) United States of America

The fair use doctrine codified under Section 107 of the US Copyright Act, 1976 comprises of the four-factor test including testing the purpose and character of use, nature of the work, amount of the work used and effect of the work on the market to decide whether the use is 'fair'. This doctrine is relied upon very frequently by the AI developers in the US to justify data scraping works. Since the works in the public domain are free for use, using them for training purposes poses no threat to copyright(Atkinson, 2025). Often times, this use is termed transformative. For instance, the court in the Bartz caseopined that Bartz use of copyrighted material in order to train the Claude AI model was transformative in nature comparing it to a reader tuned-writer model. (Bartz v. Anthropic PBC, 3:24-cv-05417, (N.D. Cal.)).In another case, scanning of millions of books by google in order to create a searchable index was allowed (Authors Guild v. Google, Inc. No. 13-4829-cv (2d Cir. Oct. 16, 2015)). While cases such as Authors Guild et al. v. OpenAI which directly address the issue whether use of copyrighted and public domain works for training AI is fair are pending, earlier decisions suggest that the courts may allow such use particularly where training process does not reproduce the exact expressions.Such judgements provide a ground and a legal cover for AI firms to build proprietary models by using works in the public domain.

While there is no risk as per the existing legal regimes, the potential riskof enclosing the public domain works and monetizing on the same by creating proprietary models is high. AI developers can easily privatize huge chunks of the cultural content reservoir without actually licensing individual works. The absence of a sui generis database right in the U.S. further facilitates such uses and allows transforming the public domain materials into a closed training dataset(Lou, 2025).The U.S. framework promotes innovation however, has very limited scope of protection against privatization of public domain resources by creating proprietary AI models.

b) European Union

The EU framework provides for a more regulated path for data mining through the Digital Single Market Directive which permits text and data mining without permission. While Article 3 of the directive is applicable to non-commercial research, Article 4 addresses commercial entities however, provides an opt-out option to right-holders. This mechanism seeks to strike

a balance between access to work and control of the work. While in theory, it looks like public domain works can be mined freely, however, the access to digitized compilations such as digital libraries may be restricted in case the right holders exercise their right to opt out of the commercial use under Database Directive.

The EU law is based on the principle of territoriality meaning that the copyright is national and the infringement of the same must occur in the relevant jurisdiction(Dornis, 2025). However, one important feature of Generative AI models is that it can be accessed across jurisdictions. Thus, AI may be subject to national Copyright laws if it is available in the EU member state, say through a download link andoffers reproduction of the work (Dornis, 2025).This forces AI companies to either restrict certain features of their AI model in the EU, make a limited version only for EU or choose to not release some models at all in the EU.Thus, owing to the risk accompanied with the territorial rules in EU, AI companies don't allow access of certain tools trained on this public domain material to people in EU. The recent EU AI Act brings a ray of hope by imposing certain transparency obligations on AI companies regarding the use of training data such as detailed summary of the content used to train models for General-purpose AI under Section 53(1)(d). Such provisions may have a direct influence on the use of public domain works. Therefore, EU provides more legal certainty as compared to other jurisdictions. (Durantaye, 2025).

c) India

"Fair dealing' is provided under Section 52(1) of the Copyright Act, 1957 permitting only limited uses of the work such as research, private study, criticism and reporting. However, the legislation makes no explicit mention of TDM exception unlike the EU law. This creates a gray area and discourage public developers and small developers from creating training datasets and forces them to rely on the proprietary models built by large tech firms and pay them usage fees in return (Niti Aayog, n.d.). This results in monopolizing and privatizing a value layer of the 'public domain' comprising of searchable corpora, curated datasets, structured meta data, summaries etc. However, the Indian law has no provision to regulate this value layer.

Practically, AI companies may extract and privatize public domain material in India. This is not done by blocking legal access to the material but by absorbing it into the training datasets of AI and controlling how it is reused through model interfaces. This concentrates the cultural capital in the hands of a few big giants with no legal requirement by them to attribute or share the value back to the communities.

d) Japan

Article 30-4 of Japan's Copyright Act,1970 allows exploiting the works for the purpose of 'data analysis.' The definition of data analysis underis extremely broad including extraction, comparison, classification or statistical analysis of the data as long as the purpose of the same is not for 'personal enjoyment.' This clause essentially permits AI developers to mine and use large amounts of data for training their models without explicit permission. However, this exception is not applicable if it is unreasonably prejudicial to the interests of the copyright holder. Article 30-4 practically permits the AI developers to train their AI systems using copyrighted and public domain works and build

their commercial systems without paying any licensing fees. Firms can easily compile training data drawn from both public domain material and once the training process is completed, the models used become private assets even though the raw data is still a part of the public domain(Umeda, 2020). This grants the companies significant control over the cultural content. In addition to this, Japan does not have a sui generis database right and also very limited transparency obligations. Together, this regime creates favourable conditions for the large AI companies to become mediators of the public domain materials, practically enclosing the same.

POLICY AND LEGAL REFLECTIONS

1) Transparency and Data Governance

One of the very basic policy responses for AI systemsis transparency. If a model uses public domain materials, it is only fair that the sources and manner of use be traceable (European Commission, 2025). EU, in its recent AI Act has mandated General-Purpose AI model providers to publish a public summary of training content under Section 53(1)(d). Transparencyallows rights-holders, researchers and public institutions to audit and verify if the AI systems are in compliance with opt-outs, licensing terms and moral obligations. Studies show that there are systematic problems such as misattribution, poor licensing and large amounts of untraceable material in the datasets that are commonly used by the AI companies to train their AI systems (Shayne Longpre, 2024).

This data can be governed in three manners-administrative (mandatory disclosures of the source), contractual (raising the licensing standards and mandatory and provenance clauses) or technological (including blockchain or signed metadata for datasets). Enforcement mechanisms and remedies are also needed (Buick, 2025).A statutory "Public-Domain respect clause" which requires disclosure of the use made, provenance of the public domain material and a liability for non-compliance may become an initial point in the battle to protect the cultural commons. While this may not stop the commercial use of the commons, it still ensures disclosure(Alan Chan, 2023). Governance must be undertaken at an international level by WIPO and UNESCO who should set global norms for AI training-data transparencyto set global expectations and create legitimacy for rules relating to the public domain. WIPO can develop a multi-stakeholder standard such for dataset transparency and provenance. On the other hand, UNESCO can integrate these norms into recommendations on the ethics of AI (UNESCO, 2021).

2) International harmonization of TDM exceptions

As discussed in the previous section, there is no uniformity in the TDM exceptions that are provided by various jurisdictions. This increases the risk of 'data arbitrage' and regulatory gaps enabling enclosure by private entities. Legal reforms must look at harmonization of TDM exceptions by way of multilateral treaties. For instance, WIPO Standing Committee and Committee on Copyright and Related Rights (SCCR) can work together to facilitate an instrument on TDM which requires signatories to provide for non-exclusive compulsory licenses and safe harbours for TDM but only for research and non-commercial uses. Such international obligations can help in reducing data localization and preventing AI firms from exploiting regulatory gaps (Samuelson,

Privacy as Intellectual Property?, 2000).

3) Fair data-sharing policies and Cultural Rights Impact Assessments

National regulators must mandate fair data-sharing frameworks requiringAI developers to share benefits arising out of use of commons either through capacity building, funding of digitization of resources, or open access to derivative models with institutions whose materials form part of the material used for training datasets. For this purpose, public-private data trust must be set-up, where public actors compile and license the data complying with the governance rules and require benefit-sharing, attribution and reinvestment in cultural infrastructure(WIPO, 2023). Such trusts retain the bargaining power and support digitization and preservation. These trusts may also use a particular standard of provenance as a pre-condition for the grant of the license.

Regulators must also mandate AI companies to perform Cultural Rights Impact Assessments (CRIAs) before making use of the public domain material. Theseassessments evaluate how the prospective use of cultural works affect the representation, value, dignity or economic value of the source communities. Academicians often argue that integrating CRIAs into tech regulation can help in safeguarding marginalized cultures(Noelle Higgins, 2022). The results of these assessments should feed into either the licensing terms or the governance mechanisms.

4) Balancing innovation and access

The main aim of copyright law is to protect the work but only for a limited period of time so that post the protection expires, the work can be used for further innovation. Thus, legal reform related to public domain must ensure that while enclosure must be prevented, it is also important to enable innovation.

The first model in this regard could be based on conditional access while mandating transparency. Where AI systems are reliant on public domain inputs which are compiled by public institutions, there could be a requirement imposed on the AI systems for the availability of a free and open tier. Another requirement could be that the outputs which may be attributable to the inputs of the public domain, carry provenance metadata. The second model could be based on time-barred exclusivity wherein AI model developers enjoy the fruits of their investment in training the AI system for a limited period of time after the expiration of which, the derivative outputs must be shared on non-exclusive terms. This system would ensure that while the AI developers secure short-term returns for their innovation, the long-term public interest is protected (Achille, 2024).

Thirdly, 'commons preserving license terms' may be mandated by data regulators whereby access may be allowed for research, education and public interest purposes, however, benefit sharing may be mandated for commercial exploitation use. Fourthly, competition law (antitrust) authorities must step in to scrutinize vertical integration whereby AI developers enter into agreements with national libraries and museums to provide them exclusive rights over their digital archives so that no other AI developer can use the same. They must also scrutinize contractual terms meant to foreclose competition in the market which mandate cloud providers, research institutions or app developers to exclusively work for the AI model provider(Lemley, 2024). Lastly, technical remedies

must be legally recognized. In case of inclusion of an improper data into the AI system, instead of completely removing the AI system, model disgorgement may be used whereby influence of the wrongly included data is surgically removed. Courts should consider such equitable remedies which are tailored to the technical realities (Feist Publications v. Rural Telephone Service Co., 499 U.S. 340 (1991).)

5) Ethical dimensions and the global south

The end goal is fairness and not merely legality. Therefore, law must not only focus on abstract rights but also on who is benefitting, who is bearing the costs and whose culture is being used or preserved. Digitized cultural heritage originally comes from public funded archives and the main aim of these is not to make huge chunks of profit, rather is preservation of the materials and access of education and culture. Because of this the global south faces two separate harms- firstly under-digitization of the archives combined with extraction of the same by large tech companies (Andrew Prescott, 2018) and secondly, epistemological distortion happening because AI models are mostly trained in languages which are dominant on the digital archives (such as English). Therefore, AI models tend to misrepresent minority cultures quite frequently giving rise to prioritization of western epistemology(Coeckelbergh, 2018).

Ethical governance requires not just access and provenance but also benefit-sharing, local digitization and legal obligations which make sure that in case public heritage is funding commercial products, some value of the same must flow back (Shayne Longpre, 2024).Normative theorists support an "AI commons" doctrine that limits privatization in case the input data derives heavily from public domain sources. (Hacker, A legal framework for AI training data from first principles to the Artificial Intelligence Act, 2021).

CONCLUSION

New debates are emerging about the nature, purpose and vulnerability of the public domain because of the advent of AI. These debates reveal that mere legal freedom to access and use the public domain materials is insufficient to guarantee a meaning public use. The main argument of this paper is that while it is not against the copyright law to use large scale public domain materials to train the AI systems, yet it produces a deeper structural harm by converting freely available commons into proprietary computational assets. This sort of enclosure does not only emerge from legal rights but also infrastructural control including model opacity, restrictive platform terms, exclusive datasets etc. This produces a paradoxical result as the materials which should be free for everyone to use become more accessible through these systems which are owned and monetized by only a few people. This effectively creates a covering on the public domain without formally altering its legal boundaries.

The comparative analysis of the legal regimes in different jurisdictions reveal that while some frameworks such as EU's TDM exceptions and Japan's broad data-analysis exception are working towards balancing innovation and openness, none of the jurisdictions adequately address the issue of re-privatization of public domain by way of platform governance and outputs. The opacity in these models further raises the issue of non-traceability of the sources by the general public, regulators and even courts. This not only raises concerns about th access of the cultural

commons abut also raises questions regarding eh integrity of AI-generated knowledge.

Moving forward, in order for creative ecosystems to sustain, it is important that the legal and institutional norms be recalibrated. Measure such as public-domain protection clauses, mandatory datasets transparency, provenance attribution and global standards on cultural commons may be helpful to re-assert public ownership over the public domain materials. Ethically, public domain governance must also ensure reinvestment, equitable access and protection against extraction of such materials.

Lastly, it is pertinent to note that in the Age of AI it is not merely sufficient to regulate technology but also important to safeguard the democratic foundations of knowledge, creativity and cultural memory. Only when it can be ensured that the public domain materials truly remain public, can innovation coexist with justice.

REFERENCES

Bartz v. Anthropic PBC, 3:24-cv-05417, (N.D. Cal.).

Achille, A. (2024). AI Model Disgorgement: Methods and Choices. Cornell University, Arxiv.

Alan Chan, H. B. (2023). Reclaiming the Digital Commons: A Public Data Trust for Training Data. Cornell University, Arxiv.

Andrew Prescott, L. H. (2018). Archive Journal. Retrieved from Why Do We Digitize? The Case for Slow: https://www.archivejournal.net/essays/why-do-we-digitize-the-case-for-slow-digitization/

Atkinson, D. (2025). Unfair Learning: GenAI Exceptionalism and Copyright Law. Cornell University, Arxiv.

Authors Guild v. Google, Inc. No. 13-4829-cv (2d Cir. Oct. 16, 2015).

Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989). .

Boyle, J. (2003). The Second Enclosure Movement and the Construction of the Public Domain. Law and Contemporary Problems, 66.

Boyle, J. (2008). The Public Domain: Enclosing the Commons of the Mind. New Haven and London: Yale University Press.

Buick, A. (2025). Copyright and AI training data—transparency to the rescue? Journal of Intellectual Property Law and Practice, 182-192.

Casey, M. A. (2020). Fair Learning. Texas Law Review, 99.

Caterina Sganga, C. G. (2025). An EU Copyright Framework for Research . JIPITEC, 312.

Caterina Sganga, C. G. (2025). An EU Copyright Framework for Research . JIPITEC, 312.

Christopher Dyer, 2. (2012). Conflict in the landscape: The enclosure movement in England, Landscape History. Landscape history (Taylor and Francis), 21-33.

Coeckelbergh, M. (2018). AI and Epistemic Agency: How AI Influences Belief Revision and Its Normative Implications. Social Epistemology .

Cohen, J. (2012). Configuring the Networked Self. Yale University Press.

Deazley, R. (2006). Rethinking Copyright History, Theory, Language. Northampton: Edward Elgar Publishing.

Deazley, R. (2006). Rethinking Copyright History, Theory, Language. Northampton: Edward Elgar Publishing.

Dornis, T. W. (2025). Generative AI, Reproductions Inside the Model, and the Making Available to the Public. International Review of Intellectual Property and Competition Law, 909-938.

Durantaye, K. D. (2025). Control and Compensation. A Comparative Analysis of Copyright Exceptions for Training Generative AI. International Review of Intellectual Property and Competition Law, 737-770.

Elkin-Koren, M. P. (2020). Accountability in Algorithmic Copyright Enforcement. Stanford Technology Law Review.

Elmahjub, E. (2025). The Algorithmic Muse and the Public Domain: Why Copyright's Legal Philosophy Precludes Protection for Generative AI Outputs. Computer L. & Sec. Rev.

European Commission. (2025, July 24). Retrieved from https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-c

Feist Publications v. Rural Telephone Service Co., 499 U.S. 340 (1991)..

G.C. Coggins, C. F. (2002). Federal Public Land and Resources. Foundation Press.

Gay, E. F. (1905). The Inclosure Movement in England. Publications of the American Economic Association, Papers and Proceedings of the Seventeenth Annual Meeting. American Economic Association.

Gervais, D. (2020). The Machine as Author. IOWA Law Review, 2053.

Gillespie, T. (2018). Custodians of the internet. Yale University Press.

Hacker, P. (2021). A legal framework for AI training data from first principles to the Artificial Intelligence Act. Law. Innovation and Technology .

Hacker, P. (2021). A legal framework for AI training data-from first principles to the Artificial Intelligence Act. Law, Innovation and Technology, 257-301.

Huang, H. (2009). On Public Domain in Copyright Law. Frontiers Law China, 179.

Huang, S. a. (2023). Generative AI and the Digital Commons. Cornell University, arxiv.

Lemley, M. A. (2024). HOW GENERATIVE AI TURNS COPYRIGHT UPSIDE DOWN . Science and Technology law Review, 21.

Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.

Lessig, L. (2001). Internet Archive. The Future of Ideas-The fate of the commons in a connected world. New York: Internet Archive.

Lessig, L. (2004). Free Culture. New York: The Penguin Press.

Lindsay, G. G. (2018). Public Rights: Copyright's Public Domains. Cambridge University Press.

Litman, J. D. (1990). The Public Domain. Emory Law Journal, 965-1023.

Lou, C. (2025). Develop-Fair Use for Artificial Intelligence: A Sino-U.S Copyright Law Comparison based on the Ultraman, Bartz v. Anthropic and Kadrey v. Meta Cases Ultraman, Bartz, and Kadrey. Cornell University, Arxiv.

Niti Aayog. (n.d.). Retrieved from https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

Noelle Higgins, D. F. (2022). Enhancing Access to Digital Culture for Vulnerable Groups: The Role of Public Authorities in Breaking Down Barriers. Int J Semiot Law, 18.

Rose, C. M. (2003). Romans, Roads, and Romantic

Creators: Traditions of Public Property in the Information Age. Law & Contemporary problems , 92.

Sajan, J. (2022). The Constricting Boundaries of Public Domain: Analysing the ramifications of restricted access in the digital epoch. IP Bulletin, 35.

Samuelson, P. (2000). Privacy as Intellectual Property? Stanford Law Review, 1125-1173.

Samuelson, P. (2024). Fair Use Defenses in Disruptive Technology Cases. UCLA Law Review, 1484.

Shayne Longpre, R. M.-M. (2024). A large-scale audit of dataset licensing and attribution in AI. Nature Machine Intelligence, 975-987.

Uhlir, J. H. (2003). Contractually Reconstructed Research Commons for Scientific Data in a Highly Protectionist Intellectual Property Environment. Law and Contemporary Problems, 318.

Umeda, Y. (2020). Japan's copyright reforms for data-driven innovation. WIPO Magazine, 12-18.

UNESCO. (2021). Retrieved from Recommendation on the Ethics of Artificial Intelligence: https://unesdoc.unesco.org/ark:/48223/pf0000373434

Weyl, D. S. (2021). We Forum. Retrieved from https://www.weforum.org/agenda/2021/06/the-case-for-the-digital-commons/

WIPO. (2023). Retrieved from Artificial Intelligence and Intellectual Property: https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence/index

Zuboff, S. (2019). The Age of Surveillance Caitalism . Public Affairs.

REGULATING LANTANA CAMARA: A LEGAL ANALYSIS WITH SPECIAL REFERENCE TO DEEPOR BEEL IN ASSAM

-Dr. Gyanashree Dutta[1]
-Dr. Upankar Chutia[2]

ABSTRACT

Lantana camara, an invasive alien plant species introduced during the colonial period, has become one of the most ecologically disruptive species in India, causing widespread degradation of terrestrial and wetland ecosystems. Its rapid proliferation, allelopathic properties, and resistance to natural predators have resulted in extensive displacement of native flora, alteration of soil composition, and loss of habitat for wildlife. This paper presents a legal analysis of the regulatory framework governing the control and management of Lantana camara, with a particular focus on Deepor Beel, a Ramsar-designated wetland located in Assam. Deepor Beel, already under severe stress from urban encroachment, solid waste dumping, and industrial runoff, faces additional ecological threats due to the spread of Lantana camara in its catchment and buffer zones, which has contributed to reduced biodiversity, altered hydrological cycles, and the fragmentation of wildlife corridors, particularly affecting the movement of elephants and wetland birds.

The research examines the existing statutory and institutional mechanisms addressing invasive species, including the Biological Diversity Act, 2002, the Wildlife (Protection) Act, 1972, the Forest Conservation Act, 1980, and the Wetlands (Conservation and Management) Rules, 2017, as well as national biodiversity action plans and management strategies. The research identifies critical gaps, such as the lack of a standalone national legislation specifically targeting invasive alien species, insufficient coordination between the Ministry of Environment, Forest and Climate Change, State Forest Departments, and Biodiversity Management Committees, and limited scientific monitoring and data-driven eradication strategies. Judicial interventions, including directions from the Supreme Court and National

Green Tribunal emphasizing ecosystem integrity and the public trust doctrine, are reviewed to assess their practical impact on controlling Lantana Camara (an invasive species) in ecologically sensitive regions like Deepor Beel.

Through its focused case analysis, the paper argues that the management of Lantana camara requires a multi-tiered governance approach integrating ecological science, community participation, and legally enforceable restoration mandates. The research proposes establishing region-specific invasive species management plans, incentivizing removal and ecological restoration, and empowering local communities through biodiversity management committees for continuous monitoring and adaptive management. Strengthening these mechanisms is essential not only for biodiversity conservation but also for protecting the cultural, ecological, and livelihood significance of wetlands like Deepor Beel.

KEYWORDS: *Biological Diversity Act 2002, Deepor Beel, Invasive Alien Species Management, Lantana camara, Wetland Conservation.*

[1]*Associate Professor, School of Law, Dayananda Sagar University, Bengaluru,*

[2]*Associate Professor, School of Law, Dayananda Sagar University, Bengaluru,*

I. INTRODUCTION

Background

Invasive Alien Species (IAS) have appeared to be one of the most widespread and inadequately handled hazards to the environment during this twenty-first century, and one of the main drivers hindering biodiversity and eco-system degradation and disintegration across this planet(Sakachep & Rai, 2021). These species result in complexities like displacement of indigenous species, eco-system disturbance, a decrease in agricultural productivity, and change within natural landscapes. The scenario is more disastrous in the case of India due to its high level of eco-diversity and lack of efficient controls on this issue. Among the many species of plants acting as an invader to Indian ecosystems, Lantana camara has emerged to be one of the most harmful to this environment. This species is originally an ornamental plant introduced to India during British colonization, which has spread across millions of hectares of forested land, natural grasslands, agricultural belts, and is gradually replacing wetlands within this unique ecosystem(Chakraborty et al., 2023).Ecological traits present in Lantana camara make it one of the most difficult species to control. The species' ability to grow vegetatively at such a rapid rate, facilitated by its strong resprouting mechanism, helps it to outcompete other species that are already stressed due to disturbance(Wittenberg & Cock, 2001).The species has strong allelopathic effects, which aid it in suppressing germination and growth of native species already present within habitats by releasing biochemical compounds. Lantana's propensity to form impervious thickets hampers animal migration routes, limited access to herbivorous vegetation, and influences micro-habitats required by fauna. The species also increases fire intensity within forests by contributing to increased combustible organic matter, resulting in an endless cycle promoting its dissemination. Lantana camara is thus one of those species that not only alters terrestrial ecosystems but is also responsible for exerting pressure onadjacent wetlands that depend on connectivity across ecological habitats, hydrological processes, and vegetation integrity(Kumar et al., n.d.).

Research Problem

Deepor Beel (Dipor Bil) is located to the southwest of Guwahati, within the Kamrup (Metro) district of the state of Assam, and is one of the largest wetlands in Northeastern India. The wetland covers 4,000 hectares in extent within its larger landscape and 414 hectares within its notified sanctity area and is recognized as a part of the natural drainage system within the Brahmaputra River basin. Hydrologically, Deepor Beel is sustained by many small streams, rainy runoff, and the Basistha and Kalmani Rivers, making this wetland a crucial part of the floodplain landscape. Geomorphologically, its shallow water bodies, swampy areas, and grasslands with periodic flooding provide a very rich source for different habitats.

Deepor Beel is known for its significance to ecosystems and notified for its importance to wetlands, and was identified as a wetland of international importance on 19th August, 2002, under the Ramsar Convention. At the national level, Deepor Beel is protected under the Deepor Beel Wildlife Sanctuary, which comes under the Wildlife (Protection) Act, 1972, signifying the importance of conservation to maintain biodiversity in Assam for posterity. It acts as a vital wintering-

breeding ground for many regional and migrating bird species, both resident and migratory such as Spot-billed Pelican, waterfowl, Lesser Adjutant Stork, Greater Adjutant Stork, and Purple Swamphen. Further, Deepor Beel is home to varied fish species, amphibians, reptiles, and aquatic vegetation making biologically very productive.

Deepor Beel wetland is also known to offer other vital ecological services. Acting as a natural river buffer, it helps to mitigate floods in the city of Guwahati. The wetland is also utilized by the communities living around it to generate income. These activities include fishing, grazing during seasons, and harvesting aquatic vegetation.

Despite being a legally recognized wetland and having such significance to nature, Deepor Beel is actually being subjected to very adverse human influences. Over the years, it has experienced visible reduction in area because of unorganized urbanization and invasion into its boundary and surrounding regions to build residential and agricultural land. The contamination generated from sewage discharge and leakage from the Boragaon dumpsite has seriously affected Deepor Beel's water quality, which is hazardous to nature and human life. The building of roads, rail tracks, and other development schemes has led to discontinuity between habitats, disturbance to hydrological regimes, and increased deposition within Deepor Beel(Das & Duarah, 2013).

Lantana camara has shown rapid growth, especially around the higher perimeter regions surrounding Deepor Beel, where it has invaded regions characterized by degraded forests and semi-dry regions. The increased growth of this species has limited natural vegetation growth, reduced grazing land for elephants and other herbivorous species, and modified wetland features required by wetland-dependent bird species. The introduction to native vegetation species hampers natural ecosystems, compromising the Ramsar Agreement to preserve natural wetland features. The growing nature of Lantana camara threatens biodiversity loss and reduced resilience to climate change stressors within Deepor Wetland.

Despite these pressing ecological risks, there is currently a disorganized and unsatisfactory legal structure to contend with and counter these effects of alien species like Lantana camara within Indian law. A comprehensive, specific statute solely dealing with controlling, regulating, eradicating, and monitoring such exotic, harmful plant species like Lantana camara is currently absent. The present scenario regarding annexing a specific statute is covered inadequately by The Biological Diversity Act, 2002, The Environment (Protection) Act, 1986, The Forest (Conservation) Act, 1980, The Wildlife (Protection) Act, 1972, and Wetlands (Conservation & Management) Rules, 2017. These statutes merely deal generally with controlling and regulating exotic species to some extent. Sometimes specific regulations contain no provision to remove such species, while other statutes merely ignore such species.

Owing to the sensitive nature of Deepor Beel and, simultaneously, the widespread prevalence achieved by Lantana camara within its environment, there arises a pressing need to discuss the legal aspects pertaining to IAS management. This paper attempts to analyze the present legal management structure devised within

India's environmental legislations to effectively control Lantana camara and assess to what extent such legislations work towards safeguarding ecologically sensitive wetlands such as Deepor Beel. This paper strives to arrive at interventions required within these gaps to effectively manage IAS.

OBJECTIVES OF THE STUDY

1. To understand the effect of Lantana camara on the natural ecosystem found in Deepor Beel.
2. To analyze the ecological aspects contributing to the quick spread of Lantana camara in and around Deepor Beel.
3. To examine the existing Indian laws related to handling invasive species like Lantana camara.
4. To analyze and provide suggestions regarding any gaps in laws and policies which could help in controlling/ managing Lantana Camara in Deepor Beel in Assam.

HYPOTHESIS

Present laws regarding environmental issues in India are insufficient to regulate, control, or manage effectively the spread of Lantana camara in environmentally sensitive areas like Deepor Beel in Assam.

RESEARCH METHODOLOGY

The study adopts a doctrinal methodological approach, which involves an in-depth analysis of statutory provisions, regulations, policies, and judicial pronouncements on managing invasive species in India.

Secondary sources like research articles, government reports and Ramsar documents on Deepor Beel are examined to analyze the biotic effects, gaps in law, and policy responses to conservation.

LANTANA CAMARA: BIOLOGY AND ECOLO - GICAL EFFECTS

Lantana camara is perennial, grows in thickets, which have the capability to outcompete herbs, young trees, and grass. Some of the most crucial points to be discussed in regard to these weeds include:

1. Lantana camara grow in such invasive ways that they outcompete other plants, such as natural ground flora, to overpower them. Eventually, they also stop trees from growing, as seedlings require light, space, and nutrients to grow, which these plants do not provide due to its dense growth(Sarma et al., 2019).
2. Allelopathic effects may inhibit other species' germination to varying degrees because of chemical leachates.
3. The dense thickets formed by Lantana can elevate fuel intensity, which can affect fire frequency or intensity, particularly within wetland-side ecosystems on land.
4. Effect on Faunal Assemblages: The displacement of natural vegetation affects bird and amphibian feeding and breeding habitats, while dense thickets may obstruct migration routes.
5. Difficulty in Management: Vegetative growth rate of lantana Camara is fast, with high productivity of seeds and resprouting after being cut.

These ecological factors imply that any legal or administrative measure to control the species should themselves be proactive, persistent, and appropriately financed because Lantana Camara possesses such potent qualities to regenerate itself by root suckers, invade and occupy cleared land quickly, and form long-lived persistent weed banks(Singh et al., 2018).

CONSERVATION STATUS OF DEEPOR BEEL

The above factors have cumulatively led to a definite attenuation in the integrity of the natural environment, which encompasses degradation due to loss of native vegetation cover, reduced water-holding capacity, and reduced numbers of specific bird and fish species(Choudhury et al., 2017). The further invasion by exotic weed species, such as Lantana camara adds to this degradation. Being aware of these hazards, state administration, conservation organizations, and research organizations have established a number of action plans and conservation programs including wetland restoration proposals, Integrated Management Plans, and biodiversity surveys. Though these proposals contain specific approaches to controlling pollutions, managing catchments, clearing weeds, and community-driven conservation programs, their implementation remained patchy due to institutional gaps, funding, and other land use priorities. As such, Deepor Beel is still an ecologically sensitive and management-intensive area.

LEGAL AND POLICY INSTRUMENTS PERTINENT TO INVASIVE SPECIES AND WETLANDS IN INDIA

1. International obligations (Ramsar Convention)

Being a Ramsar site, there are particular duties of "wise use" and conservation on the part of India with respect to Deepor Beel. The Ramsar Convention is such an international instrument which imposes on a contracting state like India to manage this wetland to preserve its nature and to make reports to the Ramsar Secretariat about any change. This is both an opportunity and a mechanism, but lacks implementation on its own.

2. Central legislation and rules

The main national laws which relate to controlling Lantana Camara on wetlands include:

i.The Biological Diversity Act, 2002 (BDA): The Act is focused on the conservation and sustainable use of biological diversity and fair sharing of its benefits. The BDA gives State Biodiversity Boards and Biodiversity Management Committees (BMC) at the village level the ability to manage biological diversity. Although it is not directly geared toward the management of invasive species, but rather can have its goals and mechanisms uses to manage invasive species.

ii. Wetlands (Conservation and Management) Rules, 2017: These rules, notified under the Environment (Protection) Act, prescribe the establishment of state wetland authorities and management plan preparation, boundary delimitation, and regulating activities that harm wetlands. These rules are one of the main instruments to take up Deepor Beel and other wetlands because they contemplate comprehensive management and participation by local communities. The rules are more guidance documents and rely on state capacity to implement.

iii. Environment (Protection) Act, 1986; Water (Prevention & Control of Pollution) Act, 1974; and Wildlife Protection Act, 1972: These Acts offer other regulatory mechanisms on issues pertaining to pollution control and harmful activities within protected zones, which can aid in wetland protection.

3. National plans and guidance on invasive species

The National Biodiversity Action Plan and other strategic documents, such as those dealing with IAS like Lantana Camara identify this issue as a challenge and discuss management approaches that incorporate prevention, early detection, and control. The strategic

documents also identify research, capacity building, and community engagement as vital building blocks to manage IAS.

4. The role of tribunals and courts

The National Green Tribunal (NGT) and the High Courts have emerged as active forums to ensure wetland protection and enforcement. The NGT's function to dispose of environment cases swiftly and judicial pronouncements can force state authorities to draw up management plans, remove invasion, and clean up pollution, which can prove useful to deal with species invasion issues where these are viewed as factors detracting from natural qualities. The recent interest shown by NGT regarding Deepor Beel is one such example that illustrates the role performed by NGT to trigger state actions.

5. State level institutions and plans (Assam)

The wetland management structure in Assam is comprised of entities such as the Assam State Wetlands Authority, Assam State Pollution Control Board, forest and fisheries departments, and specific site management authorities for Deepor Beel wetlands. Action plans developed specific to Deepor Beel contain aspects such as weed management, catchment management, and prevention of pollution, though gaps exist during implementation. Some specific plans to manage Deepor Beel include weed management.

DEEPOR BEEL - PRESENT IMPLEMENTING BODIES, MEASURES, AND THEIR ENFORCEMENT

The action plans developed for Deepor Beel, such as the Integrated Management Plan (IMP) and Wetland Conservation and Management Rules-based site-specific plans, and recommendations given by expert committees, list out a series of interventions that can be implemented to deal with regulating invasive species like Lantana Camara(Vila et al., 2011). These generally include baseline mapping of the invasives, mechanical and manual controls, management of biomass(Sharma, 2019), restoration with native vegetation species, generating alternative livelihood opportunities or Fishery Zones to decrease ecological impact, and catchment management measures to avoid disturbance to habitats, which ultimately lead to increased growth of invasives. A majority of these also stress upon involvement of local stakeholders, specifically fishing communities.

Practically, there have been weed clearing exercises, patrolling, and surveillance exercises conducted periodically by relevant authorities such as the Forest Department, State Wetland Authority, and district administration, including partnerships with NGOs and higher institutions. Mechanical weed clearing exercises have been carried out occasionally, including manual scrub cutting, particularly after the monsoon seasons when weed growth is high. There have also been initiatives to mark wetland boundary demarcation, put up signage, and conduct restoration planting(Pysek et al., 2012).

Despite this, there are still inadequate outcomes on the ground due to a range of structural, budgetary, and governance factors. The issue of invasion, both informal settlements and commercial activities, is still hindering wetland boundary integrity, thereby contributing to Lantana camara(Sharma & Raghubanshi, 2010) and other exotic species spreading effortlessly. The Boragaon dumpsite, which is located above this wetland, has pertinent effects on this

wetland due to dumpsite input into the wetland, alteration of habitat, and resulting leachate contamination. Budgeting and funding, particularly those that relate to monitoring this wetland ecologically and manage exotic species, tend to fluctuate but rather have short-term approaches.

Further, institutional fragmentation, whereby several agencies share duties but there is no nodal agency, has reduced the effectiveness of enforcing these rules. The failure to standardize monitoring approaches and link scientific studies to on-field implementation is also contributing to poor management outcomes.

The NGT, during recent years, has remained an important factor in highlighting the degradation occurring at Deepor Beel. Acting on suo motu cognizance of alleged pollution and degradation, NGT has called upon the Assam state administration, city administration, and Wetland Authority to file comprehensive affidavits and take immediate measures to initiate long-pending actions with regards to restoration. The said interventions by the higher judiciary reflect the state's understanding and recognition about Deepor Beel's fragile state of environment and restoration obligations owed to this wetland. Notably, this developing judicial oversight provides an opportunity to improve the management of invasive species. With a rationalized and appropriately financed program reflecting NGT guidelines, Deepor Beel could initiate a organized management plan incorporating both management of invasive species and development programs to restore habitats and remove contaminants. However, this requires definitions on jurisdiction, budgeting, and long-term oversight to ensure that Lantana camara and other invasive species are prevented rather than causing damage to Deepor Beel's environment.

LEGAL AND GOVERNANCE GAPS PERTAINING TO REGULATING LANTANA CAMARA IN WETLANDS (SPECIFIC TO DEEPOR BEEL)

An examination of thestatutory framework and sitesituationsindicates a number of persistent gaps between what is required and what is achieved. They are:

1.Fragmented administrative duties: There are overlapping administrative duties concerning wetlands, forest, and pollution control authorities along with local administrative bodies and biodiversity boards, but there is no lead agency to take care of eradicating invasive species.

2. Lack of compulsory action plans for management of invasive species: Though management plans are required by Wetlands Rules, they donot include strategies for managing invasive species such as Lantana camara. This results in differences within management plans implemented across different wetlands.

3. Lack of legal recognition as a separate object of administration regarding IAS: The existence of central laws like BDA ensures protection of biodiversity, but may not necessarily involve specific funding mechanisms to address IAS. There is policy guidance at a higher level, but there is limited legal support to make their control compulsory.

4. Flawed enforcement against main causes of invasion: The main drivers which trigger the invasion are incursions, landfilling, and hydrological modifications in Deepor Beel wetland ecosystems. The present strict regulations to avoid these sources of

invasion are not appropriately enforced. The involvement of NGT shows that there is a sense of legal concern, but administrative implementation is crucial. Laws do not typically incorporate funding mechanisms to support long-term eradications, nor community mechanisms via Biodiversity Management Committees or other entities.

5. Data and monitoring gaps: The control of IAS requires mapping, monitoring, and research. Though there is a call to this within national frameworks, there is no systematic monitoring at site level.

COMPARATIVE AND BEST-PRACTICE APPROACHES (BRIEF OVERVIEW)

Throughout different parts of the globe, best practices on how to deal with an invasive species like Lantana camara have arisen out of a mix of legal, biologically informed, and social approaches. Globally, countries which have been making positive progress towards dealing with this issue generally start with informed legal and institutional frameworks, which entail having one governing body tasked with controlling invasive species, having specific management strategies at each site, and a strategic inclusion of managing invasive species into any general nature protection laws. These frameworks are accompanied by dedicated funding reserves over sets of years rather than annual clearing missions(Vila et al., 2011).

Best practices also incorporate integrated management approaches. An example is how countries like Australia and South Africa deal with pampas grass by incorporating mechanical uprooting, strategic chemical use, controlled burns, and, wherever scientifically proven and safe - biological controls(Hulme, 2006). The aim is not only to remove the above-ground vegetation but to inhibit any new growth while allowing native vegetation to recover. The most effective interventions have occurred in areas from which vegetation has been removed while taking on initiatives for ecological restoration, such as native plant or species re-planting, soil conservation, and biogeochemical cycles or monitoring methods to detect changes in composition and ecological functionality.

Best practices incorporate community engagement. These projects, depending on community knowledge, with incentives, and management actions conditional on livelihood opportunities, have observed better compliances. For instance, in Africa and Southeast Asia, various species of Lantana are used to make handicrafts, furniture, briquettes, and compost, thereby creating sustainable resource utilization and adopting community ownership.Community engagement is also crucial to fill governance gaps, particularly state capacity constraints, and to ensure sustainability during management.

Within the Indian scenario, there have been pilot initiatives and state missions, such as those observed within Kerala, Karnataka, and Punjab, where it has been shown that organized and time-scaled elimination programs can contain Lantana spread with sufficient resource support and community involvement. Yet, it is apparent that successful biophysical restoration is a long-term endeavor, very much dependent on long-term monitoring and synchronization with socio-economic factors within affected communities.

RECOMMENDATIONS

A. Legal and institutional reforms

1. Make "Invasive Species Management Plan"(ISMP)

compulsory in wetland management plans. In this regard, there has to be a change in state implementation guidelines or policy interventions from Ministry of Environment, Forest and Climate Change (MoEFCC).

2. Nominate one lead agency for ground-level management of invasive species in Deepor Beel, preferably in the form of an overall coordinating cell, with leadership from the State Wetland Authority, and participants from Forest Departments, Assam Pollution Control Board, urban bodies, panchayati bodies, and BMCs. It needs to have official status to issue directions on management, with overall coordination on finance.

3. The Biological Diversity Act's local institutions, or BMCs, have to be utilized operationally. BMCs must be given official powers to co-manage removal or restoration projects for invasive species. They will provide legitimacy to community contributions, sharing benefits in biomass use, and inputs from traditional knowledge.

4. Enforce anti-encroachment, anti-pollution directions with IAS objectives together. Appeals to courts or tribunals like NGT could be made for issuing joint directions for closure or rehabilitation of illegal landfill inputs and removal of invasive species. Recently, NGT's concern for Deepor Beel shows judicial readiness to pass such orders.

B. Legal Instruments for Enhanced Implementation

1. Issue policy guidelines on ISMP through state-based policies on Wetlands Rules, with ISMP compliance necessary for state and central funds. These guidelines could be in the form of notifications from the State Wetland Authority.

2. Frame orders enforcing the public trust and statutory duties. Pursue orders from courts incorporating removal of unlawful activity with management of invasive species.

3. It is important to make sure to report any information regarding changes in ecological character due to invasive species through appropriate Ramsar mechanisms for wetland changes.

C. Operational measures (technical and social)

1. Implement progressive mechanical removal, restoration planting, and then monitoring IAS. Mechanical removal should proceed with immediate follow-through with native plantings to preclude re-invasion, with multiple-year monitoring. Seed banks or nurseries for propagule production are also to be provided.

2. Discover biologically safe controls only on scientifically sound principles: Every biologically controlled organism must meet rigorous testing for risk before being approved to excludenon-target effects.

3. Establish livelihood opportunities from removal of biomass: A value chain generated from conversion of Lantana into charcoal, crafts, or compost could generate incentives for their removal, with income opportunities for the community, tied to BMCs and local bodies.

4. Ensure stable, multiple-year financial support: National and state level programs, including dedicated wetland conservation funds, could allocate multiple-year support to ISMPs in their respective countries. These could be based on removal and restoration targets.

5.Mapping, Monitoring, and Collaborative Research: Encourage bi-annual mapping for invasive biota and ecological indicators for Deepor Beel, while

collaborating with regional universities for research contributions to adaptive management.

CONCLUSION

From the above, one could note that there is not only a biological threat, but there is also a governance challenge being posed by Lantana camara. The laws in India, such as international obligations (The Ramsar Convention), laws regarding wetlands (Wetlands Rules), laws for biodiversity (BDA), have equipped themselves with tools that could lead to positive changes. However, there are some gaps in each institutional level with regards to funding, institutional understanding on invasives, and engagement with communities that hamper productive outcomes.

Deepor Beel, being a Ramsar site threatened by pollution, invasion, and vegetation alteration, is one such high priority instance where implementing legal obligations to an ISMP (Invasive Species Management Plan) is very important. This can be achieved through improvements to the legal system (requiring ISMPs to be mandatory), a specific coordinating mechanism, strengthened legal capacity to engage civil society on an equal footing, funding tied to performance, and implementation leverage through tribunals and bureaucracies acting together.

Regarding Assam, there is a need to ensure that the regulation of Lantana camara is handled comprehensively, including assigning clarity to agency responsibility, formulating specific management strategies concerning exotic species, and allocating resources toward restoration. The involvement of local communities, particularly those that depend on wetlands, within uprooting, monitoring, and utilization initiatives can enhance compliance and make it more affordable. Recent judicial engagement, particularly NGT interventions, present a chance to consolidate an effective management strategy by the state.

Finally, it can be said that Lantana camara management at Deepor Beel Wetland needs to be perceived within the purview of Assam's overall commitment to wetlands conservation and climate change resilience. The future sustainability and protection of this unique wetland environment will depend on improving these aspects to make this wetland more resilient to any kind of danger.

REFERENCES:

1. Sakachep, Z. K., & Rai, P. K. (2021). Influence of invasive alien plants on vegetation of Hailakandi district, Assam, North-East, India. Indian Journal of Ecology, 48(1), 261-266. https://indianecologicalsociety.com/wp-content/themes/ecology/volume_pdfs/48(1)_removed%20(1)-43.pdf

2. Chakraborty, S. K., Sanyal, P., & Ray, R. (2023). Pollution, environmental perturbation and consequent loss of wetlands. In Wetlands ecology (pp. 521-582). Springer. https://doi.org/10.1007/978-3-031-09253-4_8

3. Wittenberg, R., & Cock, M. J. W. (Eds.). (2001). Invasive alien species: A toolkit of best prevention and management practices. CAB International. https://doi.org/10.1079/9780851995694.0000

4. Kumar, S., Rahman, S., Nasreen, S., Akhtar, W., Kalita, A., & Hazarika, B. (n.d.). Ecological disruption in Assam: A review of key invasive plants and their impacts on biodiversity, ecosystem, socio-economy and livelihood. Current World Environment. https://www.cwejournal.org/vol3no3/pecological-disruption-in-assam-a-review-of-key-invasive-plants-

and-their-impacts-on-biodiversity-ecosystem-socio-economy-and-livelihoodp

5. Das, K., & Duarah, P. (2013). Invasive alien plant species in the roadside areas of Jorhat, Assam: Their harmful effects and beneficial uses. International Journal of Engineering Research and Applications, 3(5), 353-358.

6. Sarma, N., Shankar, U., & Mao, A. A. (2019). An assessment of the invasive flora of Amchang Wildlife Sanctuary in the Kamrup District of Assam, India. Pleione, 13, 326.

7. Singh, M. K., Verma, P., Bharti, A., & Kumar, R. (2018). Forest invasive species: A serious threat to native species in forest habitat of Assam, India. Archive of Life Science and Environment, 2(1), 97-104.

8. Choudhury, M. R., Deb, P., & Singha, H. (2017). Status of invasive plant species in the dry savanna grasslands of Rajiv Gandhi Orang National Park, Assam. International Journal of Ecology and Environmental Sciences, 43(3), 245-250.

9. Vila, M., Espinar, J. L., Hejda, M., Hulme, P. E., Jarošík, V., Maron, J. L., Pergl, J., Schaffner, U., Sun, Y., & Pyšek, P. (2011). Ecological impacts of invasive alien plants: A meta-analysis of their effects on species, communities and ecosystems. Ecology Letters, 14(7), 702-708. https://doi.org/10.1111/j.1461-0248.2011.01628.x

10. Sharma, V. (2019). Weed as underutilized bio-resource and management tool: A comprehensive review. Waste and Biomass Valorization, 10(7), 1795-1810. https://doi.org/10.1007/s12649-018-0212-2

11. Pysek, P., Jarošík, V., Hulme, P. E., Pergl, J., Hejda, M., Schaffner, U., & Vilà, M. (2012). A global assessment of invasive plant impacts on resident species, communities and ecosystems: The interaction of impact measures, invading species' traits and environment. Global Change Biology, 18(5), 1725-1737. https://doi.org/10.1111/j.1365-2486.2011.02636.x

12. Sharma, G. P., & Raghubanshi, A. S. (2010). How Lantana invades dry deciduous forest: A case study from Vindhyan highlands, India. Tropical Ecology, 51(2), 305-316.

13. Vila, M., Espinar, J. L., Hejda, M., Hulme, P. E., Jarošík, V., Maron, J. L., Pergl, J., Schaffner, U., Sun, Y., & Pyšek, P. (2011). Ecological impacts of invasive alien plants: A meta-analysis of their effects on species, communities and ecosystems. Ecology Letters, 14(7), 702-708. https://doi.org/10.1111/j.1461-0248.2011.01628.x

14. Hulme, P. E. (2006). Beyond control: Wider implications for the management of biological invasions. Journal of Applied Ecology, 43(5), 835-847. https://doi.org/10.1111/j.1365-2664.2006.01227.x

THE ROLE OF AI ARTIFICIAL INTELLIGENCE IN THE CONSUMER PROTECTION ACT OF 2019

Mr. Mahesh S Betasur*

ABSTRACT

The Consumer Protection Act, 2019 represents a significant reform in India's consumer law framework, emphasizing faster redressal, enhanced product liability standards, and accountability in e-commerce. With the rapid growth of digital markets, Artificial Intelligence (AI) has emerged as a transformative tool in strengthening the Act's objectives. AI enables real-time detection of unfair trade practices, misleading advertisements, and defective products through automated data analytics. It supports the Central Consumer Protection Authority (CCPA) by enabling intelligent monitoring of online marketplaces, identifying patterns of consumer fraud, and facilitating evidence-based investigations. AI-driven chatbots and grievance-handling systems can enhance consumer access to information and reduce delays in complaint resolution. Further, AI can assist in comparative pricing, consumer awareness campaigns, and risk assessment in product liability cases. At the same time, the integration of AI raises concerns related to algorithmic bias, data privacy, transparency, and accountability of digital platforms, which must be addressed to ensure fairness. Overall, AI has the potential to significantly advance consumer welfare, strengthen regulatory oversight, and enhance the effectiveness of the Consumer Protection Act, 2019, provided that its use is guided by ethical and legal safeguards

I. INTRODUCTION

The Consumer Protection Act, 2019 ("CPA 2019") replaced the Consumer Protection Act, 1986, to address the challenges posed by modern commerce, especially digital and e-commerce markets. The Act introduced new provisions including the establishment of the Central Consumer Protection Authority (CCPA), stricter liability standards for defective goods, and mechanisms for expeditious dispute resolution.

With the rapid expansion of e-commerce and digital marketplaces, the complexity of consumer transactions has increased, necessitating the adoption of advanced technological solutions. Artificial Intelligence (AI) has emerged as a pivotal tool capable of augmenting consumer protection by enabling real-time monitoring, predictive analytics, and automated grievance handling.

AI applications range from detecting fraudulent advertisements to assisting in product recalls, risk assessment, and consumer awareness initiatives. However, the integration of AI into consumer protection frameworks also raises concerns regarding privacy, transparency, and accountability of algorithms. This paper examines the role of AI under CPA 2019 and its potential to enhance consumer rights while maintaining ethical safeguards.

2. CONSUMER PROTECTION ACT, 2019: KEY PROVISIONS

*Head of Department, School of Law, Kristu Jayanti (Deemed to be University) Bengaluru, Karnataka

2.1 Central Consumer Protection Authority (CCPA)

Section 10 of CPA 2019 empowers the CCPA to investigate consumer complaints, initiate proceedings, and regulate unfair trade practices. AI can aid the CCPA by:

- Monitoring online marketplaces for deceptive advertising.
- Detecting patterns of consumer fraud through predictive analytics.
- Automating the collection and analysis of evidence for enforcement proceedings.

2.2 Product Liability and E-Commerce Accountability

Product Liability under Consumer Protection Act, 2019

The Consumer Protection Act, 2019 introduced a comprehensive framework for product liability, which holds manufacturers, service providers, and sellers accountable for defective goods or services that cause harm to consumers. Key provisions include:

Section 2(34): Defines a defect as any fault, imperfection, or shortcoming in quality, quantity, potency, purity, or standard of goods or services.

Section 84: Establishes product liability action, allowing consumers to claim compensation for harm caused by defective products.

Liability is strict, meaning the manufacturer or seller can be held responsible even without negligence, if the product is defective and causes injury.

AI's Role in Product Liability:

Artificial Intelligence can strengthen the enforcement of product liability by:

Predictive Analytics: AI systems can analyze product defect patterns from customer complaints, quality audits, or e-commerce reviews to identify potentially hazardous products before widespread harm occurs.

Automated Monitoring: AI-powered tools can continuously monitor online marketplaces for the sale of defective or counterfeit goods, alerting authorities or sellers to prevent consumer harm.

2. E-COMMERCE ACCOUNTABILITY UNDER CONSUMER PROTECTION ACT, 2019

The Act recognizes the unique challenges of e-commerce, especially with online marketplaces acting as intermediaries. Key aspects include:

Section 2(35): Defines consumer to include any person buying goods or services through e-commerce platforms.

Section 2(36): Includes e-commerce operators within the definition of service providers.

Section 17 & 18: Imposes responsibilities on e-commerce platforms to ensure transparency, authenticity, and safety of products, and to provide mechanisms for grievance redressal.

AI's Role in E-Commerce Accountability:

AI enhances e-commerce accountability by:

Detection of Unauthorized or Counterfeit Sellers: AI algorithms can analyze seller data, track unusual patterns, and flag non-compliant sellers, as seen in cases like Amazon India v. Amway India.

Automated Complaint Resolution: AI-powered chatbots and case management systems can quickly address consumer grievances, reducing delay in the dispute resolution process.

Risk Assessment: AI models can evaluate transaction data and product reviews to identify high-risk products that may violate consumer rights.

Regulatory Compliance: AI can help e-commerce operators monitor compliance with labeling, product standards, and mandatory disclosures as required

under the Act.

3. Integration of AI in Consumer Protection

By combining product liability enforcement and e-commerce accountability, AI transforms consumer protection in the digital age:

It proactively prevents harm by identifying defective products or unsafe practices.

It ensures transparency in online marketplaces.

It reduces litigation time through automated evidence collection, monitoring, and dispute management.

2.3 Consumer Dispute Redressal Mechanism

CPA 2019 establishes a three-tier consumer dispute redressal system (District, State, and National Commissions). AI can improve efficiency by:

- Utilizing chatbots for preliminary complaint registration.
- Streamlining case documentation and evidence collation.
- Prioritizing cases based on severity and potential consumer impact.

3. ROLE OF AI IN STRENGTHENING CONSUMER PROTECTION

The Role of Artificial Intelligence in Strengthening Consumer Protection

The rise of Artificial Intelligence (AI) has significantly reshaped the landscape of consumer protection, especially in an era dominated by e-commerce, digital transactions, and online services. AI technologies, including machine learning, natural language processing, and predictive analytics, are increasingly being deployed to safeguard consumer interests, enforce product liability, and ensure accountability among manufacturers, service providers, and online marketplaces. The Consumer Protection Act, 2019 (CPA 2019) in India emphasizes timely redressal of consumer grievances, strict liability for defective products, and regulation of e-commerce platforms. AI emerges as a crucial enabler in realizing these objectives efficiently and proactively.

1. AI and Product Liability

Product liability is a central pillar of consumer protection under CPA 2019, which holds manufacturers and service providers accountable for harm caused by defective goods or services. Section 84 of the Act explicitly allows consumers to seek compensation for injury or damage caused by defective products, even in the absence of negligence. AI strengthens this framework by enabling predictive monitoring and risk detection. For instance, AI algorithms can analyze customer complaints, product reviews, and warranty claims to detect recurring defects in electronics, pharmaceuticals, or nutritional supplements. Early identification of defective products prevents widespread harm, reduces litigation, and ensures timely recall.

A relevant illustration of product accountability in digital commerce is the case of ***Amazon India v. Amway India Enterprises Pvt. Ltd. (2020)*** [1]. In this case, Amway alleged that unauthorized sellers on Amazon were offering counterfeit products, potentially harming consumers. The Delhi High Court underscored that e-commerce platforms must exercise due diligence to prevent the sale of defective or unauthorized goods. AI-based monitoring tools can automate the detection of such violations, ensuring that marketplaces comply with the obligations outlined under CPA 2019 and uphold product safety.

2. AI and E-Commerce Accountability

[1] *MANU/DE/0311/2020*

The proliferation of online marketplaces has introduced unique challenges for consumer protection. Under Sections 2(36) and 17–18 of CPA 2019, e-commerce operators are classified as service providers and must guarantee product authenticity, safety, and transparent grievance redressal mechanisms. AI significantly enhances e-commerce accountability by:

Monitoring Seller Behavior: Machine learning models can identify suspicious sellers, unauthorized distribution channels, or counterfeit listings.

Consumer Complaint Management: AI-driven chatbots and automated case management systems streamline grievance handling, enabling faster resolution.

Fraud Detection: AI can analyze transaction patterns to identify potential scams, false advertisements, or misleading pricing practices.

The ***Anvar P.V. v. P.K. Basheer (2014)***[2] case, while primarily concerning electronic evidence, underscores the importance of digital data authenticity. AI systems can ensure that electronic records, transaction logs, and online consumer complaints are accurate, verifiable, and admissible in consumer courts, facilitating effective enforcement of CPA 2019.

3. AI for Regulatory Oversight and Consumer Protection

Regulatory bodies like the Central Consumer Protection Authority (CCPA) benefit from AI in conducting data-driven interventions. AI tools can analyze consumer feedback, social media trends, and online reviews to detect unfair trade practices, misleading advertisements, or non-compliant product standards. This proactive approach allows regulators to target enforcement actions efficiently, enhancing transparency and trust in the market.

Furthermore, AI enhances consumer awareness. Recommendation systems and alert mechanisms can notify users about product recalls, safety warnings, or fraudulent sellers. This proactive dissemination of information empowers consumers to make informed decisions and exercise their rights effectively under CPA 2019.

4. Case Laws Illustrating Consumer Protection under CPA 2019

4.1 **Amazon India v. Amway India**

Amway India challenged Amazon India for allowing third-party sellers on its platform to sell unauthorized and potentially counterfeit Amway products. Amway contended that these sales violated its distribution agreements and misled consumers, while Amazon argued that it was only a marketplace intermediary and not directly responsible for the sellers' actions. The Delhi High Court examined the scope of intermediary liability under Section 79 of the Information Technology Act, 2000, and emphasized that while e-commerce platforms are not absolute insurers of product authenticity, they must exercise due diligence to prevent the sale of counterfeit or unauthorized goods. The Court highlighted that under the Consumer Protection Act, 2019, platforms have an obligation to ensure consumer rights are protected, and failing to act on complaints or implement robust monitoring could attract liability. This case is significant as it clarified the responsibilities of online marketplaces in India, reinforcing that platforms must establish mechanisms to verify product authenticity, prevent counterfeit sales, and provide effective consumer grievance redressal, thereby strengthening both consumer

[2] *(2014) 10 SCC 473'*

[3] *https://www.scconline.com/blog/post/2020/07/30/advertisement-to-misleading-advertisement-horlicks-ltd-v-zydus-wellness last visited on 10/12/2025, 7.00pm*

protection and brand integrity in the digital marketplace. Horlicks Ltd. v. Zydus Wellness[3] The case addressed misleading health claims in advertising. AI can detect similar misleading marketing strategies across digital platforms, aiding the CCPA in timely enforcement actions.

4.3 Anvar P.V. v. P.K. Basheer[4]

The Supreme Court of India dealt with the admissibility of electronic evidence under the Indian Evidence Act, 1872, particularly in criminal cases. The appellant challenged a conviction relying on electronic records such as CD-ROMs and printouts as evidence. The Court held that electronic records are admissible only if they comply with the conditions laid down under Section 65B of the Evidence Act, which requires a certificate authenticating the electronic record. The judgment clarified that without a proper Section 65B certificate, electronic evidence cannot be admitted, even if the original device is produced. This ruling is landmark as it strengthened the legal framework for digital evidence in India, ensuring authenticity and reliability, and has since been widely cited in cases involving cybercrime, e-commerce disputes, and consumer protection matters involving electronic transactions.

5. Challenges and Ethical Concerns in AI Integration

5.1 Algorithmic Bias

AI systems may inherit biases from training data, leading to unfair treatment of certain consumer groups. Biased algorithms in complaint prioritization or risk assessment could undermine consumer protection.

5.2 Data Privacy and Security

The use of AI requires large datasets, often containing sensitive consumer information. CPA 2019 interacts with Information Technology Act, 2000, necessitating strict safeguards to prevent misuse of personal data.

5.3 Transparency and Accountability

AI decisions must be explainable. Black-box algorithms pose challenges for accountability in regulatory investigations. Section 10 of CPA 2019 mandates transparent enforcement, which can conflict with opaque AI systems.

6. Global Perspectives: AI in Consumer Protection

Global Perspectives: Artificial Intelligence in Consumer Protection

The global marketplace has undergone a paradigm shift in recent years, largely driven by digitalization, e-commerce, and the integration of Artificial Intelligence (AI) into everyday commercial transactions. AI has emerged as a transformative tool in enhancing consumer protection, enabling regulators, businesses, and consumers themselves to manage risks associated with product defects, unfair trade practices, misleading advertising, and digital fraud. Across the world, legal frameworks and regulatory authorities are increasingly recognizing the potential of AI to strengthen consumer rights, enforce accountability, and improve transparency in commerce.

AI and Consumer Protection: A Global Overview

Consumer protection globally encompasses ensuring product safety, promoting fair trade practices, and safeguarding consumer data and privacy. With the rise of e-commerce, online marketplaces, and AI-driven personalized services, traditional frameworks have faced challenges in keeping pace with technological developments. AI technologies—particularly machine learning, natural language processing, and predictive analytics—have begun addressing these gaps by

[4] *2014 AIR SCW 5695*

enabling real-time monitoring, predictive risk assessment, and automated grievance redressal systems.

6.1 United States

In the United States, AI is increasingly integrated into regulatory compliance and consumer protection enforcement. The Federal Trade Commission (FTC) has emphasized the role of AI in detecting unfair or deceptive business practices, ensuring product safety, and protecting consumers in digital marketplaces. For instance, in ***FTC v. Amazon (2023)***[5], the FTC scrutinized Amazon for enabling third-party sellers to sell defective or counterfeit products on its platform. While the case focused on intermediary accountability, it highlighted the potential role of AI tools in monitoring seller behavior, analyzing consumer complaints, and preventing harm before it occurs. AI-powered algorithms can flag high-risk sellers or transactions, thereby complementing regulatory oversight and enhancing consumer safety.

6.2 European Union

The European Union (EU) has been at the forefront of integrating AI within consumer protection and digital governance frameworks. The General Data Protection Regulation (GDPR, 2018) ensures that consumer data is protected in AI-driven services, while the upcoming Artificial Intelligence Act (AIA, 2024) aims to establish a comprehensive regulatory framework for AI systems, including their deployment in consumer-facing applications. AI is particularly utilized in:

Detecting misleading advertisements and unfair commercial practices: Machine learning models can scan digital platforms for deceptive marketing campaigns.

Monitoring product compliance: AI tools help identify defective products or non-compliant services sold online.

Supporting consumer dispute resolution: AI-driven online dispute resolution (ODR) systems facilitate faster grievance redressal.

A landmark instance is the EU's enforcement against e-commerce platforms hosting counterfeit goods, where AI monitoring systems have been recommended to track high-risk sellers and prevent consumer harm proactively.

6.3 United Kingdom

The UK's Competition and Markets Authority (CMA) has increasingly recognized AI's role in ensuring marketplace fairness and consumer protection. AI-powered analytics assist in identifying price-fixing, misleading advertising, and data-driven unfair practices. In cases involving online marketplaces like Amazon and eBay, AI tools were deployed to monitor seller compliance, detect anomalies in pricing patterns, and identify counterfeit or unauthorized goods. These initiatives underscore the growing reliance on AI to uphold both consumer rights and fair competition in digital commerce.

6.4 Asia-Pacific Region

Countries like China, Singapore, and South Korea are integrating AI into consumer protection enforcement and e-commerce regulation. In China, the E-Commerce Law (2019) obliges online marketplaces to ensure product authenticity, traceability, and timely redressal of consumer complaints. AI systems are extensively used for:

Real-time monitoring of counterfeit goods.

Tracking product defects through consumer reviews

[5] *No. 2:23-cv-01495, U.S. District Court for the Western District of Washington*

and complaint patterns.

Implementing AI-driven chatbots for instant grievance resolution.

Similarly, Singapore's Consumer Protection (Fair Trading) Act leverages AI for monitoring online trading platforms, ensuring transparency, and identifying fraudulent activities.

7. Recommendations for Effective AI Integration

1. Ethical AI Guidelines: Adopt AI frameworks ensuring fairness, transparency, and non-discrimination.
2. Data Governance: Strengthen consumer data protection in compliance with IT Act and upcoming Data Protection Bill.
3. Human Oversight: AI should complement, not replace, human decision-making in consumer forums.
4. Regulatory Sandbox: Encourage experimentation with AI tools under controlled conditions for monitoring consumer protection outcomes.
5. Continuous Monitoring and Evaluation: Assess AI effectiveness in identifying unfair trade practices, complaint resolution, and consumer education.

8. Conclusion

AI holds transformative potential for strengthening the objectives of the Consumer Protection Act, 2019. By enabling real-time monitoring, predictive analytics, and automated grievance handling, AI can enhance regulatory efficiency, consumer welfare, and market transparency. However, ethical and legal challenges, including algorithmic bias, data privacy, and accountability, must be addressed to ensure fairness. A balanced approach integrating AI technology with human oversight, ethical frameworks, and robust regulatory mechanisms can significantly advance consumer protection in India's rapidly evolving digital marketplace.

MIGRATION-RELATED VULNERABILITIES AND LEGAL SAFEGUARDS FOR WOMEN IN JAMMU & KASHMIR

Ms. Ankita[1]

ABSTRACT

Migration Jammu and Kashmir has evolved in layers of conflict brought on displacement, economic migration, seasonal labour migration and social relocation which have evolved certain implication on women. Women become more vulnerable to migration due to gender aspect of migration which includes economic marginalisation, social security, low mobility, vulnerability to informal labour markets, loss of property rights with the possibility of gender based violence. The given proposed study, titled as Migration-Related Vulnerabilities and Legal Safeguards against Women in Jammu and Kashmir, relies upon the socio-legal method of the investigation of the ways in which migration changes the rights, agency, and welfare of women in the region.

To understand how migrant women live and what constitutes the structural issues that they face, the studies analyze different categories of migrant women: displaced women, labour migrants, seasonal migrants, internally displaced persons and cross-regional migrants. It takes into account the adequacy of the legal safeguard, including constitutional and human rights guidelines, labour laws, and welfare rights and entitlements, and plans initiated or state-based. Legal and administrative changes had also been adopted since 2019, and are discussed just to examine how it had impact on the legal status of women, their access to justice and their socio-economic mobility.

Despite the elaborate regime of the law structure, the loopholes in practice have been determined by the administrative disintegration cases, social-cultural constraints, temporal deficiency in legal literacy and underperforming institutionalization. The paper also recommends that the legislation such as the Protection of Women against Domestic Violence Act labor laws, social security, and welfare initiatives have significant protection, but fails to consider the intersectional problems of migrant women.

This paper has concluded that effective legal protection of migrant women in Jammu & Kashmir should be done using gender-responsive policies, better legal literacy, delivery of welfare services to migrant women, and enhanced mechanisms of institutional support in the same. These structural gaps should be brought up as part of the means to foster gender justice and enable women to savor their rights in the rapidly evolving socio-political context.

Keywords: *Migration, Women Rights, Jammu and Kashmir, Gender-Based Vulnerabilities, Displacement, Socio-legal Study, Legal Safeguards, Gender justice.*

I. INTRODUCTION

The issue of migration in Jammu & Kashmir (J&K) has been historically conditioned by a peculiar mixture of the political conflict with the geographical isolation and

[1]*Research Scholar University Of Jammu Department Of Law*

socio-economic changes. Contrary to the rest of India, J&K migration patterns are overlayed with years of insurgency, militarisation, economic under-development and non-relocation of communities living in border belts and conflict prone districts. The area has been experiencing several types of mobility: forced displacement as a result of armed conflict, seasonal movement by pastoral groups (such as the Gujjar and Bakarwal tribes) within the region, labour migration caused by unemployment, and intra-regional movement of families involved in living areas at risk (Bhan, 2013; Government of India, 2021). The intricate migration patterns have generated a unique socio-demographic contours in which most of the time it is women who suffer the instability, displacement of livelihoods and total loss of community ties.

Migration among women is different in comparison to men because of deeply-rooted socio-cultural values, gendered dichotomy of labour and structural asymmetries that restrict their locomotion, agency, and resource availability. Studies has shown that gender and migration have put women at a higher risk of economic exploitation, inadequate healthcare, social discrimination, and the violence against them in terms of gender (Jolly & Reeves, 2005; UN Women, 2019). These are then exacerbated in J&K since most women migrants belong to conflict-affected or economically disadvantaged backgrounds in which educational and work opportunities tend to be limited already. In cases whereby migration interferes with the old support systems, women tend to become increasingly subject of dependency, lower bargaining power, both at home and in accessing law or welfare services.

The socio-legal significance of researching the rights of migrant women in J&K is in the fact that it is possible to comprehend the interrelation of gender and conflict with institutional characteristics. The legal environment at J&K has been changing significantly since the reorganisation of the region in 2019, which extended the region to several central laws and welfare schemes. Although these legal reforms can transform the results of access to women rights and welfare, the lived experiences of migrant women demonstrate that there are continuous gaps on the implementation, awareness and institutional responsiveness (Ministry of Home Affairs, 2020). Laws protecting against domestic violence against women, sexual harassment of women at workplaces, and even other schemes of welfare theoretically are and should be equally applied to migrant women; however, the practical limitations include the absence of documentation, caste tribe exclusions, and during their implementation, th fragments of the administration systems prevent their effective use.

Additional gendered effects of migration are also increased by the regional specifics of J&K. The cross-border firing often leads to displacement in border districts, including Kupwara, Rajori, Poonch, Kathua, and Samba, where the families, especially women, children, and the elderly, have to move temporarily or permanently (Chowdhary, 2017). Moreover, nomadic tribal populations such as Gujjar and Bakarwal are displaced on a seasonal basis, which interferes with the quality of their healthcare, education, and welfare services, including women who are likely to use the communities locally available to them as a social and family support network (Sharma, 2019). The dismissed Kashmiri Pandits in the 1990s have also demonstrated

that women have long-term consequences on mental health, personal safety, and economic involvement through post-conflict movement (Bhan, 2013). Such multi-layered migration patterns explain why J&K can not be studied within generic migration patterns, yet since its socio-political context needs a region-based gendered analysis.

Researching on the rights of migrant women in J&K is thus important due to a number of reasons. To begin with, migrant women form one of the most socio-economically disadvantaged segments of the population which issues them access to justice due to structural and cultural barriers. Second, knowledge of their vulnerabilities assists the policymakers in developing gender-responsive migration governance, welfare delivery system, and legal interventions. Third, the existing body of J&K research in terms of conflict and security pays less attention but much to the restructuring of women legal rights, social position, and economic contribution, through migration. Close-up of this gap is necessary in developing inclusive policies in accordance with national pledges provided in the Constitution of India and with international models like the Convention to Elimination of All Forms of Discrimination Against Women (CEDAW).

This introduction preconditions the further discussion of how migration creates certain vulnerabilities of women in J&K and why the legal protection should be discussed in the framework of socio-legal, rights-based approach. In the following part, the migration patterns in J&K will be mapped and the impacts of diverse mobility forms on women in diverse socio-economic and cultural settings will be demonstrated.

2. OBJECTIVES OF THE STUDY

The proposed paper attempts to examine the multifaceted convergence of migration, gender, and law in the state of Jammu and Kashmir where a historical conflict, displacement, and socio-economic changes have had a distinct impact on the lives of women. The initial goal is to examine the gender-related vulnerabilities against migrant women in J&K, such as the economic marginalisation, social insecurity, limited mobility, lack of health services, and increased vulnerability to violence. The paper also aims at analyzing the socio-legal environment, which regulates the rights, as well as protections, which can be mounted to women regarding migration issues, evaluating both the official legal texts and the effective implementation of these texts.

The other major aim is to assess the efficiency of the constitutional guarantees, the statutory safeguards, and welfare schemes, in solving the problem of migrant women. As the J&K reorganisation occurred in 2019 and the region now is subject to the central laws, the study also focuses on determining how the post-2019 legal restructuring affects women rights, especially in regard to their property rights, welfare rights, and access to justice. Lastly, the study aims at establishing the long-standing gaps between the law and ground reality, which will provide information on the challenges in implementation, institutional limitations, and socio-cultural challenges that impede the achievement of rights of migrant women.

3. LITERATURE REVIEW

Although migration has always been an economic factor of India, migration studies have commonly been concerned with labour flows, rural to urban movement, and migration factors as mobility but with gendered

migration, women have been shown to be more mobile in relation to other individuals due to the social norms, structural inequalities and lack of access to resources (Deshingkar&Akter, 2009). Gender in the larger context of South Asia determines the influence of women on their migration, vulnerability, and capability of asserting their rights in the host societies (Nazneen& Mahmud, 2012). Such groundwork of scholarship highlights the fact that migration cannot be examined without considering the overlapping of gender, poverty, caste, and geography.

There is a body of literature in the case of Jammu and Kashmir, which associates migration with conflict, displacement and militarisation. Research indicates that over a long period of time, the region has experienced a cycle of instability, which has witnessed dislocation of border communities, pastoralism, as well as massive mass migration of the Kashmiri Pandit during the 1990s (Bhan, 2013; Bose, 2003). It has also been found that displacement due to conflicts affects aspects like family structure, puts women under emotional stress, and adds to their household and economic responsibilities (Mankotia, 2014). These texts generate the structural factors under which the vulnerabilities of migrant women occur.

Very much of the literature is devoted to tribal movement, particularly in the relation to Gujjar and Bakarwal communities in which seasonal pastoralists live. Their twice-a-year transgression across rugged landscape leads to unequal receipt of the healthcare, education, and welfare services, problems that disfavor women (Sharma, 2019; Rahi, 2014). The women in the nomadic societies have certain weaknesses in the form of inadequate reproductive healthcare, early marriages, and non-documentation, which limit their right to access the state welfare program. This scholarship brings out the necessity of policy frameworks that consider mobility as opposed to viewing livelihoods as sedentary.

The studies that explore the issue of the rights of women in J&K also indicate structural inequalities based on the social and legal systems. According to Chowdhary and Mohanty (2018), the women in the region have long been limited by property ownership, inheritance, and ability to move freely because of a strong patriarchal tradition. Despite having constitutional safeguard and national legislations set in place that protect the region, there are gaps in implementation, especially to the women who lack a stable residence or documentation. Gender-based violence in conflict zones is also associated with the underreporting pattern, inaccessibility of the justice system, and an institutional indifference (Human Rights Watch, 2019). Migrant women have such problems compounded by the fact that they usually do not have local support systems.

Since 2019, even the scholarship has turned its focus on law reorganization of J&K in aftermath of abrogation of Article 370 and 35A which repatriated all central law on the area. Analysts believe that this change has enhanced some legal rights of women particularly, regarding property and inheritance matters (Singh, 2020). Nevertheless, these researches also observe that even legal changes do not ensure substantial rights, particularly to women who are in disadvantaged socio-economic status. Structural barriers that migrant women still have to address are a lack of awareness, administrative barriers, and insufficient access to

institutions (Ministry of Home Affairs, 2020). This solidifies the disparity between the formal legal guidelines and the real access to rights.

The literature on migration and labour vulnerabilities of women in India, in general, is also available. Research demonstrates that migrant women working in the domestic area, the construction industry, and the informal labour market are being exploited and subjected to the dangerous working environment, a social insurance deficit (Sastry, 2016; ILO, 2018). When transferred to J&K, the findings correspond with the research that female labour migrants in Jammu and other cities tend to work without a contract, are subjected to harassment, and disqualified as the basis of welfare mobility and informality (Kumar, 2021). The criticality of these discussions is in the context of the ways in which national trends of migrant women exploitation overlap with the peculiarities of the situation at J&K on conflict and displacement.

Although much research has been conducted on the prevalence of conflict in J&K, gender, and displacement, there is still a shortage of literature with special attention to migration-driven vulnerabilities of women in a socio-legal context. The available literature focuses on rights of women, patterns of migration or consequences of conflicts as standalone entities without much intertwining efforts to present a consistent analysis. Literature has also been found to be inadequate on post 2019 administrative and legal reforms to date, and their influence on the access of migrant women to welfare, justice and protection processes. The latter research gap highlights the significance of conducting a detailed social-legal study that would explore the area of vulnerabilities, as well as legal protection in the specific contexts of J&K.

Generally, the literature demonstrates that although legal frameworks are in place, the socio-cultural norms, institutional loopholes, and the strain of conflict based movement impose an uphill task on the women. The results of earlier studies have formed a solid ground to the current research that aimed to tie these threads into a cohesive study on the rights of migrant women in Jammu & Kashmir.

4. RESEARCH PROBLEM AND HYPOTHESIS.

Migration in Jammu and Kashmir is a multifaceted collision between conflict-related displacement, seasonal migration, and economic migration as well as inter-regional migration. Although migration experiences the whole household, women are vulnerable in much more gendered ways that can be influenced by cultural values, restraint in movement and economic dependence as well as lack of access to legal and institutional protection. Available literature demonstrates that women in migration situations are under the increased threat of exploitation, domestic and workplace violence, loss of means of livelihood, and healthcare and welfare services. Nevertheless, even in the wake of the increased legal framework and the welfare programs in J&K, particularly, following the restructuring of the latter in 2019, migrant women are still facing an uphill climb towards their rights. Such obstacles are the absence of documentation, poor knowledge of the law, bureaucracy, under-representation in decision making and entrenched patriarchal restraint of their involvement in the political arena.

This becomes the research problem because the lives of migrant women in J&K are plagued by a mismatch

between the formal laws and their real lives. Despite the constitutional guarantees, gender-protective laws, and welfare provisions, which are currently supposed to extend to all women, the process of their application to migrant women is uneven. Little scholarly analysis has looked at how migration in particular redefines the rights of women in the particular socio-political setting of J&K, particularly given that the region has long been characterized by the conflicts, displacement, tribal migration, and increased vulnerability to the borders. This raises a serious void that is the scope of the present study to fill in a socio-legal analysis.

It is on this basis that the following hypotheses are developed to be used in this study:

H1: Migration enhances socio-cultural and institutional barriers and thus paves the way of gender based vulnerability to women in Jammu and Kashmir.

H2: Migrant women do not have sufficient realisation of rights due to insufficient implementation of existing constitutional, statutory and welfare protection.

H3: Legal restructuring after 2019 has enhanced formal legal entitlements to women in J&K but has had no significant impact on access to ground-level justice or welfare by migrant women.

5. METHODOLOGY

The chosen research methodology in the present study consists of the socio-legal, doctrinal, and analytical research approach to assess the vulnerabilities of women and the provisions related to the migration in Jammu & Kashmir. Since the topic of conflict-based mobility is sensitive and the feasibility of carrying out the fieldwork in the high-risk or remote locations is constrained, the study is based mostly on the secondary data and the existing qualitative solutions.

The methodology approach requires its doctrinal component that entails an in-depth analysis of the constitutional provisions, legislations, welfare programs, and judicial determinations on the rights of women and the protections of the migrants. This involves examining legislations like the Protection of Women against Domestic Violence Act, 2005; Sexual Harassment at Workplace Act, 2013; criminal law legislation; labour regulations and welfare systems that were in place in J&K prior to the reorganisation in 2019. Government reports, policy documents and parliamentary discussions were also checked to evaluate the scope and effects of restructuring of the law.

The socio-legal aspect aims at comprehending the lived realities of migrant women by looking at reliable secondary sources including scholarly journals, research reports, human rights records, NGO reports and census figures and government surveys. The following sources illuminated the intersection of gender, conflict, migration, and institutional effectiveness in J&K with particular emphasis on the studies concerning GujjarBakarwal migration, border displacement, conflict-related mobility, and labour migration.

These doctrinal and socio-legal findings are synthesised into the analysis method to address the hypotheses of the study and measure the gap between law and ground reality. With the triangulation of different sources and positions, the methodology can guarantee reliability and validity, as well as point out the trends of vulnerability and gaps in the system.

This is the most appropriate method to the aim of the

research, as it will enable a holistic picture of the legal framework as well as gendered migration realities in Jammu & Kashmir.

6. HYPOTHESIS

The hypotheses will be based on a question of how migration is in relation to gender, law, and institutional structure in Jammu & Kashmir. The null hypothesis (H1) is that migration is a powerful cause of gender-related vulnerabilities to women in the region. This assertion is highly supported by secondary research evidence. Conflict-related displacement has demonstrated severally that women lose access to stable livelihoods, education, and community networks whenever they migrate thus becoming more reliant upon male family members as well as the more susceptible to exploitation. Research on border migrants, internally displaced families and tribal nomadic community suggests that women often experience greater domestic loads, inadequate healthcare, and greater violence in the course of displacement or resettlement. In addition, migrant female workers in informal places of work, domestic and construction, complain of unhealthy working conditions, bullying, and social non-protection. These trends affirm that not only do these migrations transfer women to other geographical locations, but it is reducing their socio-economic capacities, which confirms H1.

The second hypothesis (H2) suggests that the constitutional, statutory and welfare protection is poorly enforced on the migrant women in J&K. An examination of the reports by the government, legal documents, and scholarly research shows that there are great gaps in the implementation. Women have legal rights of enjoyment as per the laws of the country but due to absence of their identity documents, lack of awareness skills, and inefficiency in the administration, they are often not able to have the benefits of these laws under the Constitution. As an illustration, women seasonal migrants tend to be deprived of welfare schemes as a result of being mobile whereas conflict displaced women find it hard to acquire ration tickets, residence, or property documents. Although laws such as the Domestic Violence Act or protections of labour may exist formally ensuring that bureaucratic bodies are able to intervene, actual enforcement mechanisms are poor because institutional reach is limited, agencies are uniformly understaffed and because socio-cultural interventions prevent women reporting cases of abuse. These results indicate that there is a apparent discrepancy between the legal and lived experiences, thus attesting to H2.

The third hypothesis (H3) posits that post-legal restructuring (after the abrogation of Article 370) has enhanced formularies but not ground-based access. To some extent, this hypothesis is justified. These formal rights of women have been reinforced through the extension of all the central laws to J&K particularly in the field of property, inheritance, and eligibility in welfare. A number of core plans which include social security pensions and healthcare plans are now equally enforced. But actual facts indicate that such formal advances have not totally translated into the available benefits to migrant women. Moving administrations, bureaucracy, and absence of gender sensitive governance remain to be the impediments on ground towards a real change. The migrant women especially those in the border villages or the nomadic population

are yet to experience a significant barrier in receiving healthcare, legal systems, labour, and welfare. Therefore legal restructuring has not adequately enhanced the practicalisation of the rights as it has increased the prerogatives but has not substantially justified H3.

The general trend of all three hypotheses is that, on the one hand, the migration strengthens gendered vulnerabilities, on the other hand, legal concerns exist but are poorly applied and finally, recent legal interventions have not achieved success in facilitating the environment between legal provisions and the reality of life. These conclusions highlight that there is an urgent need to have stronger, gender responsive migration governance in Jammu and Kashmir.

7. ANALYSIS & DISCUSSION

Migration in Jammu and Kashmir is not simply a demographic one but socio-political and gendered process that has taken decades of conflict and geographical weakness coupled with economic instability. Women found in migrating families face both structural disadvantages that cut across gender, class, tribe and regional instability. The subsequent exegisis uncodes the transformation of their economic status, social mores, expressed in the possibility of access to law, as well as safety and welfare, indicating the endemic divide between legislation and experience.

7.1 Economic Vulnerabilities

One of the most urgent issues facing migrant women in J&K is economic instability that, in most cases, interferes with the household sources of income and makes the family depend on irregular labour, seasonal employment, or unskilled jobs. In case of women, it is further complicated by low levels of education, absence of profession, and the social constructions that restrict them to unpaid care giving services.

Female migrant workers in the domestic labour fields, construction, brick kilns, or even in the fields of agriculture are often subjected to discrimination of wages, unpaid labour, and working under unfavorable conditions. To the larger extent that majority of these jobs are within the informal sector, women are seldom provided with written contracts, social security, maternity and healthcare services. Dependence on male earners is also amplified due to economic displacement minimizing the bargaining power of women in the household thus making them vulnerable to exploitation.

Where women of Gujjar and Bakarwal communities are concerned, migration bi-monthly denies them access to stable markets or jobs thus putting them in the clutches of poverty. In the case of displaced women of the border areas, the constant changes of the location make it impossible to continue employing or livelihood training and thus economic recovery is very tough. Migration, therefore, creates economic gaps between men and women and increases the vulnerability of women.

7.2 Social and Cultural Vulnerabilities.

Migration also changes the social settings of women dramatically as most of the time the support systems within the community are undermined and unable to provide safety, direction, and emotional support, which were traditional supports. Women migrants particularly of conflict-touched or rural origin communities find themselves in a drastic situation of losing all their social circles thus finding themselves in new environments alone.

In J&K, cultural practices still restrict the mobility of women, their freedom of decision-making, and their visibility to the world. These norms accompany families, which restrict the capacity of women to become part of the new societies or even access basic services. An example is that seasonal migrants have difficulty in ensuring the enrolment of children into schools, in anganwadi services and lack access to social programmes. Besides, cross-regional marriage migrants experience a language barrier and cultural clearing which increases isolation.

Widows, separated women and single female migrants have the greatest social vulnerability. In the absence of male guardianship, they are stigmatized, having less security and less access to welfare. Displacement aggravates mental health, trauma and anxiety within women in conflict zones, which further limits the social participation. Migration, therefore, breaks the continuity of culture and establishes patriarchal reliance.

7.3 Legal Vulnerabilities

Although there are existing laws to protect migrant women in India, the migrant women encountered sustained problems regarding their access to the justice system in J&K. There are three broad causes of legal vulnerability; no documentation, little rights awareness, and poor institutional response.

One of the most important barriers is documentation barriers. Migrant women usually have no important documents like Aadhar cards, domicile certificates, Ration cards, or the property documentation. In the absence of them, they will not be in a position to receive government schemes, make complaints and demonstrate identities in case of legal proceedings. Seasonal migration also brings a problem in documentation as a person who migrates continuously has a problem with keeping records updated.

Legal access is also impeded by the awareness gaps. Most migrant women do not know the protection of the law like the Protection of Women against Domestic Violence Act, legislation against sexual harassment, and labour codes. Fear of being stigmatised, facing reprisals or lack of faith in institutions all prevent reporting of violence even when general awareness has been created.

These issues are aggravated by institutional issues. Remote communities and border belts usually contain low police presence, understaffed legal aid centres, and a lack of agreement between departments. Nomadic people seldom find permanent institutional support on the migration paths. Combined, these aspects create a crippling discrepancy between what the law provides and their real application.

7.4 Gender-Based Violence & Violence of the students.

Migration makes women vulnerable to violence and insecurity. The economic strains, migration, and social disintegration provide the conditions under which gender-based violence is more probable and challenging to deal with.

Females in border districts who have somehow lost their homes often complain of increased cases of domestic violence as a result of stress, unemployment and isolation in temporary shelters. The migrant labour women are exposed to the threat of workplace harassment, illicit demands, and trafficking. Women in homes and remote areas also have no one to testify against abuse because they do not have a system to

report.

In the case of nomadic Gujjar-Bakarwal women, the migration paths subject them to trafficking dangers, rape, and poor living standards. Pastoral shelters or temporary settlement is hardly observed and the women are at risk. The intensity of the conflict in some of the districts is an added security issue, and women are threatened by the armed factions, security agents, or even by criminals.

The lack of trust in law enforcers, fear, and stigma are the primary causes of under-reporting, which is prevalent. This is because the justice system is not accessible to migrant women, and as such, numerous cases are not visible, only to continue intensifying violence.

Forming a partnership with a healthcare provider requires a substantial amount of time, energy, and financial resources.

7.5 Healthcare & Welfare Vulnerabilities

Migration has a very great impact on access to welfare and healthcare services. India is associated with many schemes that are related to residence, documentation or stable location, which is disturbed with migration.

Migrant women tend to have no access to:

- Molded Fetal and Reproductive Medical Care.
- Immunisation services
- Anganwadi nutrition schemes.
- Social security pensions
- MGNREGA employment
- PDS ration benefits

This means seasonal migrants may lose entitlements even when they change districts as well as displaced women in camps which use congested, unsanitary amenities to expose them to health hazards.

The cultural and logistical obstacles to access medical centers are also experienced by women especially when using a remote or mountainous path. Small numbers of female healthcare personnel, transport disparities, and ignorance about their entitlements further inhibit their entitlement to care. To most migrant women, welfare regimes are a virtual unattainable entity, regardless of being enshrined in law.

7.6 Case Study Insights

(a) Gujjar–Bakarwal Migrants

Their transhumance twice a year interferes with access to health, education and welfare. The women are the greatest affected by a lack of reproductive care, unsafe migration routes as well as deprivation of rations entitlements throughout movement.

(b) Border Area Displacement

Women that are displaced through cross-border shelling move in and out of women shelters and villages. This insecurity lowers documentation, school and healthcare access, which puts women into insecurity-dependency loops.

(c) Urban Labour Migrants at Jammu.

Women who are domestic workers or construction helpers are exploited in terms of their wages, unsafe working environments and are harassed. Whether they lack awareness, and the absence of legal contracts aggravates their vulnerability.

As demonstrated above, the gendered inequalities in J&K are aggravated through the migration process in several channels, including but not limited to economic instability, social isolation, legal exclusion, violence, and welfare deprivation. Despite the existence of laws, loopholes in implementation, the documentation and institutional back-up means that migrant women are

unable to get the best out of it. Migration thus ends up being a magnifier of vulnerability with the realization of a very marked disconnection between formal rights and realities.

8. RECOMMENDATIONS AND CONCLUSIONS.

The conflict, geography, economic instabilities, and seasonal migration combine to shape migration in Jammu & Kashmir in a complex manner. This paper identifies that women in such migration patterns are vulnerable in a multidimensional way that seriously compromises the relevant rights, safety, and access to justice. Migration impacts on both the whole family, but its effects on women are much deeper, as they are connected to deep-rooted patriarchal norms, socio-economic, and lack of institutional support. The discussion indicates that migrant women suffer economic exploitation, social seclusion, and legal marginalization, are exposed to violence, and access welfare and health services inconsistently. The application of these rights is grossly imbalanced although there are constitutional protections, statutory guarantees, and welfare schemes.

The hypotheses are tested and it is confirmed that the migration increases the vulnerability of the genders and that the legal protection even when it exists on paper is not well practiced by migrant women within the region. The legal restructuring after 2019 has broadened the official definition of rights entitled to women, though administrative changes, difficulty with documentation, and socio-cultural restrictions make access to them still limiting. This continued disconnection between the law and lived experience makes it necessary to have a more responsive and gender-sensitive framework that meets the needs of the migrant women in Jammu and Kashmir.

In a bid to fill this gap, the study proposes a number of recommendations. First, there is the need to develop gender-responsive migration policies where they should address the safety, livelihood, and documentation needs of women. Second, it is necessary to organize legal literacy programmes addressed to migrant communities (and women, in particular) to make them more aware of existing rights and protections. Third, the welfare systems should be changed in a place where welfare is portable whereby migrant women will be able to receive social security benefits regardless of the movement in the geographical locations. Fourth, women help desks, mobile legal aid clinics and community-based grievance cells are all gender-sensitive institutional mechanisms that ought to be reinforced in both rural and urban regions. Fifth, special camps to support documentation exercise must be established in areas of high migrant population as well as in the tribal migration paths to facilitate timely issues of ration cards/Aadhaar and domicile certificates.

Besides, the labour protection should be implemented more effectively since migrant women are the most susceptible in such areas as domestic work and construction. The partnership between NGOs, community networks, and government agencies can promote the monitoring and service provision. Finally, policymakers should make sure that migration governance in J&K is guided by the participation of women, and in particular displaced, tribal, and economic marginalised women to ensure that policy

consequences are based on their lived experiences.

To conclude, to guarantee real protection of migrant women in Jammu and Kashmir, effective laws, as well as, implementation, institution and consistent social support are needed. It is only then that the region is able to be oriented towards a more balanced and rights-based migration framework.

REFERENCES

Bhan, M. (2013). Counterinsurgency, democracy, and the politics of identity in India: From warfare to welfare? Routledge.

Bose, S. (2003). Kashmir: Roots of conflict, paths to peace. Harvard University Press.

Chowdhary, N. (2017). Border residents and everyday life under cross-border shelling in Jammu & Kashmir. Economic and Political Weekly, 52(13), 45–52.

Chowdhary, N., & Mohanty, B. (2018). Gender, conflict, and displacement in Jammu & Kashmir. Economic and Political Weekly, 53(12), 40–48.

Deshingkar, P., & Akter, S. (2009). Migration and human development in India. UNDP Human Development Research Paper Series, 2009/13.

Government of India. (2021). Migration in India 2020–2021. Ministry of Statistics and Programme Implementation. https://www.mospi.gov.in

Human Rights Watch. (2019). Everyone lives in fear: Patterns of impunity in Jammu and Kashmir. https://www.hrw.org

International Labour Organization. (2018). Women and men in the informal economy: A statistical picture (3rd ed.). ILO.

Jolly, S., & Reeves, H. (2005). Gender and migration: Overview report. BRIDGE/Institute of Development Studies.

Kumar, V. (2021). Urban labour migration and women workers in Jammu. Journal of Labour and Development, 9(1), 55–70.

Mankotia, A. (2014). Conflict, suffering, and the Kashmiri women's experience. Journal of International Women's Studies, 15(2), 117–129.

Ministry of Home Affairs. (2020). Annual report 2019–2020. Government of India. https://www.mha.gov.in

Nazneen, S., & Mahmud, S. (2012). Gendered politics of securing livelihoods: Migrant women in South Asia. IDS Bulletin, 43(1), 65–76.

Rahi, J. N. (2014). Tribal migrations and identity in Jammu & Kashmir. Tribal Research Bulletin, 36(2), 15–28.

Sastry, N. (2016). Women in India's informal economy: Vulnerabilities and opportunities. Indian Journal of Labour Economics, 59(3), 345–364.

Sharma, M. (2019). Pastoral nomadism and seasonal migration among Gujjar–Bakarwal tribes of Jammu & Kashmir. Journal of Himalayan Studies, 12(2), 112–130.

Singh, A. (2020). Legal transformations in Jammu & Kashmir after the abrogation of Article 370: Implications for women. Indian Journal of Public Administration, 66(4), 526–542.

UN Women. (2019). Gendered dimensions of migration: A global perspective. https://www.unwomen.org

डिजिटल निगरानी और निजता का अधिकार: राष्ट्रीय सुरक्षा एवं नागरिक स्वतंत्रताओं का संतुलन

डॉ योगेश कुमार गुप्ता
प्रोफेसर, आई.पी.इ.एम लॉ एकेडेमी,
गाज़ियाबाद

सार/ABSTRACT

डिजिटल प्रौद्योगिकियों के तीव्र विकास ने शासन, सुरक्षा और सामाजिक जीवन को अभूतपूर्व रूप से रूपांतरित किया है। इंटरनेट, स्मार्टफोन, सोशल मीडिया, कृत्रिम बुद्धिमत्ता और बड़े डेटा (Big Data) के व्यापक उपयोग के साथ डिजिटल निगरानी राज्य की एक प्रमुख नीति-साधन बनकर उभरी है। आतंकवाद, संगठित अपराध, साइबर अपराध और राष्ट्रीय सुरक्षा से जुड़ी चुनौतियों का सामना करने के लिए सरकारें निगरानी तंत्र को आवश्यक मानती हैं। किंतु यह निगरानी नागरिकों के निजता के अधिकार, अभिव्यक्ति की स्वतंत्रता और व्यक्तिगत स्वायत्तता के लिए गंभीर प्रश्न खड़े करती है। भारत में के.एस. पुट्टस्वामी बनाम भारत संघ (2017) के ऐतिहासिक निर्णय ने निजता को संविधान के अनुच्छेद 21 के अंतर्गत मौलिक अधिकार के रूप में मान्यता दी। इसके पश्चात डिजिटल निगरानी और डेटा संग्रहण से जुड़े कानूनों व नीतियों की संवैधानिकता पर गहन विमर्श प्रारंभ हुआ। यह शोध पत्र राष्ट्रीय सुरक्षा और नागरिक स्वतंत्रताओं के मध्य संतुलन की आवश्यकता का विश्लेषण करता है तथा यह प्रश्न उठाता है कि किस सीमा तक राज्य द्वारा निगरानी न्यायोचित है। अध्ययन में भारतीय विधिक ढाँचे, न्यायिक दृष्टिकोण, डेटा संरक्षण कानून तथा अंतरराष्ट्रीय मानकों का विश्लेषण किया गया है। शोध का उद्देश्य यह स्पष्ट करना है कि एक लोकतांत्रिक समाज में सुरक्षा आवश्यकताओं की पूर्ति करते हुए निजता के अधिकार की रक्षा कैसे की जा सकती है।

कीवर्ड - डिजिटल निगरानी, निजता का अधिकार, राष्ट्रीय सुरक्षा, नागरिक स्वतंत्रताएँ

I. भूमिका/INTRODUCTION

डिजिटल युग में सूचना और संचार प्रौद्योगिकी ने मानव जीवन के प्रत्येक क्षेत्र को प्रभावित किया है। शासन व्यवस्था, कानून प्रवर्तन, बैंकिंग, स्वास्थ्य, शिक्षा और सामाजिक संपर्क अब डिजिटल माध्यमों पर निर्भर होते जा रहे हैं। इस परिवर्तन के साथ राज्य और निजी संस्थानों के पास नागरिकों से संबंधित विशाल मात्रा में डेटा एकत्र करने और उसका विश्लेषण करने की क्षमता विकसित हुई है। डिजिटल निगरानी इसी संदर्भ में एक महत्त्वपूर्ण अवधारणा के रूप में सामने आती है।

डिजिटल निगरानी का तात्पर्य नागरिकों की ऑनलाइन गतिविधियों, संचार, लोकेशन डेटा, वित्तीय लेन-देन तथा डिजिटल व्यवहार की निगरानी से है। सरकारें इसे राष्ट्रीय सुरक्षा, सार्वजनिक व्यवस्था, अपराध नियंत्रण और आतंकवाद निरोध के लिए आवश्यक मानती हैं। भारत जैसे विशाल और विविधतापूर्ण देश में, जहाँ आंतरिक और बाह्य सुरक्षा चुनौतियाँ विद्यमान हैं, निगरानी को एक निवारक एवं अन्वेषणात्मक उपकरण के रूप में देखा जाता है।

हालाँकि, डिजिटल निगरानी के बढ़ते दायरे ने निजता के अधिकार पर गंभीर प्रभाव डाला है। निजता केवल व्यक्तिगत गोपनीयता तक सीमित नहीं है, बल्कि यह व्यक्ति की गरिमा, स्वायत्तता और स्वतंत्र निर्णय लेने की क्षमता से जुड़ी हुई है। निरंतर निगरानी का भय नागरिकों के व्यवहार को नियंत्रित कर सकता है, जिससे अभिव्यक्ति की स्वतंत्रता और लोकतांत्रिक सहभागिता कमजोर हो सकती है।

भारतीय संविधान में निजता का अधिकार स्पष्ट रूप से उल्लिखित नहीं था, परंतु पुट्टस्वामी निर्णय के बाद इसे मौलिक अधिकार के रूप में मान्यता प्राप्त हुई। इस निर्णय ने यह स्थापित किया कि किसी भी प्रकार की राज्यीय निगरानी

को वैध उद्देश्य, आनुपातिकता और विधिक प्रक्रिया की कसौटी पर खरा उतरना होगा।

यह अध्ययन डिजिटल निगरानी और निजता के अधिकार के मध्य संतुलन की समस्या का विश्लेषण करता है। यह इस बात पर केंद्रित है कि राष्ट्रीय सुरक्षा की आवश्यकताओं को पूरा करते हुए नागरिक स्वतंत्रताओं की रक्षा कैसे सुनिश्चित की जा सकती है।

2. अध्ययन के उद्देश्य (Objectives of the Study)

इस अध्ययन के प्रमुख उद्देश्य निम्नलिखित हैं:

1. डिजिटल निगरानी की अवधारणा, स्वरूप और विकास का विश्लेषण करना।
2. भारतीय संविधान के अंतर्गत निजता के अधिकार की प्रकृति और विस्तार को समझना।
3. राष्ट्रीय सुरक्षा के संदर्भ में राज्य द्वारा डिजिटल निगरानी की आवश्यकता और औचित्य का परीक्षण करना।
4. डिजिटल निगरानी से उत्पन्न नागरिक स्वतंत्रताओं पर प्रभावों का मूल्यांकन करना।
5. राष्ट्रीय सुरक्षा और निजता के अधिकार के बीच संतुलन स्थापित करने हेतु विधिक एवं नीतिगत उपायों का सुझाव देना।

3. साहित्य समीक्षा (Review of Literature)

डिजिटल निगरानी और निजता पर वैश्विक स्तर पर व्यापक साहित्य उपलब्ध है। वेस्टिन (1967) ने निजता को व्यक्तिगत सूचना पर नियंत्रण के अधिकार के रूप में परिभाषित किया। लायन (2001) ने निगरानी को आधुनिक समाज का एक अनिवार्य अंग बताया, जो शक्ति और नियंत्रण से जुड़ा हुआ है।

भारतीय संदर्भ में, पुट्टस्वामी बनाम भारत संघ पर आधारित विद्वानों के लेखों ने निजता को मौलिक अधिकार के रूप में स्थापित करने की संवैधानिक व्याख्या प्रस्तुत की है। भाटिया (2018) ने डिजिटल भारत पहल के अंतर्गत डेटा संग्रहण की वैधता पर प्रश्न उठाए।

अंतरराष्ट्रीय स्तर पर यूरोपीय संघ का सामान्य डेटा संरक्षण विनियमन (GDPR) निजता संरक्षण का एक सशक्त मॉडल प्रस्तुत करता है। सोलोवे (2011) ने निगरानी और निजता के बीच संतुलन के लिए जवाबदेही और पारदर्शिता पर बल दिया।

हालाँकि, अधिकांश साहित्य या तो सुरक्षा को प्राथमिकता देता है या निजता को, जबकि दोनों के मध्य व्यावहारिक संतुलन पर सीमित अध्ययन उपलब्ध हैं। यह शोध इसी अंतर को भरने का प्रयास करता है।

4. अध्ययन का महत्व (Significance of the Study)

यह अध्ययन डिजिटल युग में लोकतांत्रिक शासन के समक्ष उत्पन्न एक महत्त्वपूर्ण विधिक एवं सामाजिक समस्या को संबोधित करता है। डिजिटल निगरानी के बढ़ते उपयोग के कारण नागरिकों के मौलिक अधिकारों पर पड़ने वाले प्रभावों को समझना आवश्यक हो गया है।

यह शोध नीति-निर्माताओं, विधि-निर्माताओं, न्यायपालिका और शिक्षाविदों के लिए उपयोगी सिद्ध हो सकता है। अध्ययन राष्ट्रीय सुरक्षा और नागरिक स्वतंत्रताओं के मध्य संतुलन की आवश्यकता को रेखांकित करता है तथा यह स्पष्ट करता है कि बिना पर्याप्त सुरक्षा उपायों के निगरानी लोकतांत्रिक मूल्यों को कमजोर कर सकती है।

5. अनुसंधान पद्धति (Research Methodology)

यह अध्ययन द्वितीयक स्रोतों पर आधारित है। इसमें विधिक ग्रंथों, संवैधानिक प्रावधानों, न्यायिक निर्णयों, शोध पत्रों, सरकारी रिपोर्टों और अंतरराष्ट्रीय दस्तावेजों का विश्लेषण किया गया है। तुलनात्मक और विश्लेषणात्मक पद्धति अपनाई गई है ताकि भारतीय ढाँचे की तुलना अंतरराष्ट्रीय मानकों से की जा सके।

6. डिजिटल निगरानी और निजता का अधिकार

डिजिटल निगरानी राज्य को अपराध रोकथाम और सुरक्षा सुनिश्चित करने में सहायता प्रदान करती है, परंतु इसके अंधाधुंध उपयोग से अधिकारों का हनन संभव है। भारत में टेलीग्राफ अधिनियम, आईटी अधिनियम और हालिया डेटा संरक्षण कानून निगरानी के लिए विधिक आधार प्रदान करते हैं। न्यायपालिका ने समय-समय पर यह स्पष्ट किया है कि निगरानी केवल विधि द्वारा स्थापित प्रक्रिया के अनुसार और आनुपातिक रूप से ही की जा सकती है। फिर भी, पारदर्शिता और स्वतंत्र निगरानी तंत्र की कमी एक बड़ी चुनौती बनी हुई है।

डिजिटल निगरानी निजता के अधिकार के साथ तभी संगत हो सकती है जब यह कानूनी, आवश्यक, आनुपातिक हो, और इस पर कड़ी निगरानी हो; जब ये सुरक्षा उपाय मौजूद नहीं होते हैं, तो यह नागरिक स्वतंत्रता और लोकतांत्रिक जवाबदेही को कमजोर करती है, भले ही इसे राष्ट्रीय सुरक्षा के नाम पर सही ठहराया जाए। समकालीन मानवाधिकार कानून आतंकवाद जैसे वैध उद्देश्यों के लिए लक्षित निगरानी को स्वीकार करता है, लेकिन अंधाधुंध या मनमानी सामूहिक निगरानी को अस्वीकार करता है जो अभिव्यक्ति की स्वतंत्रता को बाधित करती है और संस्थानों में विश्वास को कम करती है।

एक मौलिक अधिकार के रूप में निजता: निजता के अधिकार को मानवाधिकारों की सार्वभौम घोषणा के अनुच्छेद 12 और नागरिक और राजनीतिक अधिकारों पर अंतर्राष्ट्रीय संधि के अनुच्छेद 17 में मान्यता प्राप्त है, जो निजता, परिवार, घर और पत्राचार में मनमाने या गैर-कानूनी हस्तक्षेप को प्रतिबंधित करते हैं। राज्यों का यह भी सकारात्मक कर्तव्य है कि वे ऐसे कानूनी ढांचे बनाएं जो व्यक्तियों को सार्वजनिक अधिकारियों और निजी संस्थाओं दोनों द्वारा निजता के उल्लंघन से प्रभावी ढंग से बचाएं।

राष्ट्रीय सुरक्षा और निगरानी शक्तियां: सरकारें आतंकवाद, गंभीर अपराध और साइबर खतरों को रोकने के लिए डिजिटल निगरानी को आवश्यक बताती हैं, यह तर्क देते हुए कि संचार डेटा और मेटाडेटा तक पहुंच से खुफिया जानकारी और प्रतिक्रिया क्षमताओं में सुधार होता है। हालांकि, बड़े पैमाने के कार्यक्रमों (जैसे PRISM-शैली के संचालन और थोक डेटा संग्रह) के अनुभव से पता चलता है कि राष्ट्रीय सुरक्षा के दावे ठोस खतरों से कहीं आगे बढ़ सकते हैं, जिससे निरंतर निगरानी सामान्य हो जाती है।

मुख्य कानूनी परीक्षण: वैधता, आवश्यकता, आनुपातिकता: अंतर्राष्ट्रीय और संवैधानिक अदालतें तेजी से तीन-भाग वाले परीक्षण को लागू कर रही हैं: कोई भी निजता-प्रतिबंधित उपाय स्पष्ट रूप से कानून पर आधारित होना चाहिए, राष्ट्रीय सुरक्षा जैसे वैध उद्देश्य के लिए सख्ती से आवश्यक होना चाहिए, और अधिकारों पर इसके प्रभाव में आनुपातिक होना चाहिए। बहुत व्यापक या अंधाधुंध डेटा संग्रह, कमजोर लक्ष्यीकरण मानक, और अस्पष्ट "राष्ट्रीय सुरक्षा" परिभाषाएं आमतौर पर इन परीक्षणों में विफल हो जाती हैं क्योंकि वे एक विशिष्ट खतरे से निपटने के लिए आवश्यक लोगों की तुलना में कहीं अधिक लोगों को प्रतिबंधित करती हैं।

नागरिक स्वतंत्रता और लोकतंत्र के लिए जोखिम: सामूहिक या अपारदर्शी निगरानी अभिव्यक्ति की स्वतंत्रता को बाधित कर सकती है, असहमति को रोक सकती है, और राजनीतिक और सामाजिक आंदोलनों में भागीदारी को हतोत्साहित कर सकती है, खासकर पत्रकारों, कार्यकर्ताओं और हाशिए पर पड़े समूहों के बीच। लगातार डेटा संग्रह और प्रोफाइलिंग दुरुपयोग, कार्य विस्तार, और भेदभाव के जोखिमों को भी बढ़ाती है, जिससे शक्ति भारी मात्रा में राज्य और निजी मध्यस्थों की ओर स्थानांतरित हो जाती है और मुख्य लोकतांत्रिक मूल्यों को कमजोर करती है।

सुरक्षा और अधिकारों को संतुलित करने के लिए सुरक्षा उपाय: अधिकांश समकालीन विद्वता और न्यायशास्त्र सुरक्षा आवश्यकताओं को नागरिक स्वतंत्रता के साथ सामंजस्य बिठाने में मदद करने वाले सुरक्षा उपायों के एक समूह पर सहमत हैं: सटीक और सार्वजनिक निगरानी कानून, पूर्व न्यायिक प्राधिकरण, स्वतंत्र और अच्छी तरह से संसाधन वाले निगरानी निकाय, सख्त डेटा-न्यूनतमकरण और प्रतिधारण सीमाएं, और व्यक्तियों के लिए प्रभावी उपचार। पूरक उपायों में मज़बूत डेटा-प्रोटेक्शन कानून, एन्क्रिप्शन और सुरक्षित स्टोरेज के लिए सपोर्ट, ट्रांसपेरेंसी रिपोर्टिंग, और निगरानी प्रथाओं की सिविल सोसाइटी और संसदीय स्तर पर लगातार जांच शामिल है।

i-डिजिटल सर्विलांस की अवधारणा, प्रकृति और विकास

डिजिटल सर्विलांस का मतलब है डिजिटल टेक्नोलॉजी के ज़रिए व्यक्तियों के डेटा की व्यवस्थित निगरानी, संग्रह और विश्लेषण, जिसमें लक्षित (विशिष्ट संदिग्ध) और बड़े पैमाने पर (व्यापक आबादी) दोनों तरह के दृष्टिकोण शामिल हैं। इसके मूल में, इसमें व्यवहार, संचार और स्थानों को ट्रैक करने के लिए क्लोज्ड-सर्किट टेलीविज़न (CCTV), चेहरे की

पहचान, डेटा माइनिंग और स्पाइवेयर जैसे उपकरणों का उपयोग शामिल है। डेविड लियोन जैसे विद्वानों द्वारा परिभाषित, यह प्रभाव, प्रबंधन या सुरक्षा के लिए व्यक्तिगत विवरणों पर केंद्रित ध्यान देने की एक "सामाजिक प्रथा" है, जो अक्सर शक्ति की गतिशीलता और प्रतिरोध के साथ जुड़ी होती है। इसकी प्रकृति दोधारी है: यह सुरक्षा बढ़ाने में सक्षम बनाती है, जबकि AI के माध्यम से गोपनीयता के क्षरण, सामाजिक नियंत्रण और पूर्वाग्रहों को बढ़ाने का जोखिम भी पैदा करती है।

इसका विकास 20वीं सदी के मध्य से शुरू होता है, जब 1940 के दशक में औद्योगिक निगरानी के लिए एनालॉग CCTV सिस्टम पेश किए गए थे, जो 1960 के दशक तक व्यापक शहरी उपयोग में विकसित हो गए। 20वीं सदी के अंत में डिजिटल बदलाव एक महत्वपूर्ण मोड़ था: डिजिटल वीडियो रिकॉर्डर (DVR) ने VHS टेप की जगह ले ली, जिससे स्केलेबल स्टोरेज और रीयल-टाइम विश्लेषण संभव हुआ। 1990 के दशक तक, इंटरनेट के उदय ने डेटाविलेंस को सुविधाजनक बनाया - टाइमस्टैम्प और स्थानों जैसे मेटाडेटा के माध्यम से व्यवस्थित डेटा ट्रैकिंग - जिसे 1988 में रोजर क्लार्क ने गढ़ा था। 9/11 के बाद, राष्ट्रीय सुरक्षा की अनिवार्यताओं ने इसे गति दी, जिसमें PATRIOT Act (2001) जैसे अमेरिकी कानूनों ने इलेक्ट्रॉनिक निगरानी का विस्तार किया, जिससे वैश्विक मानदंडों पर प्रभाव पड़ा।

2010 के दशक में AI और बिग डेटा के माध्यम से घातीय वृद्धि देखी गई। कंप्यूटर विज़न, जो सैन्य अनुप्रयोगों में निहित है, ने लाइव फेशियल रिकग्निशन (LFR) जैसे उपकरणों को शक्ति प्रदान की, जिन्हें सार्वजनिक स्थानों पर खतरे का पता लगाने के लिए तैनात किया गया था, लेकिन अल्पसंख्यकों की पहचान करने में त्रुटियों के लिए इसकी आलोचना की गई। एडवर्ड स्नोडेन के 2013 के खुलासों ने PRISM जैसे बड़े पैमाने पर निगरानी कार्यक्रमों को उजागर किया, जिससे "स्नोडेन विरोधाभास" पर बहस छिड़ गई - जहाँ अवैध प्रथाओं ने सुरक्षा के बहाने वैधता हासिल कर ली। 2020 के दशक में, "इंटरनेट ऑफ थिंग्स" (IoT) ने स्मार्ट फ्रिज से लेकर पहनने योग्य उपकरणों तक, रोजमर्रा के उपकरणों में निगरानी को एकीकृत किया, जिससे सार्वजनिक-निजी सीमाएँ धुंधली हो गईं। 2025 तक, AI-संचालित भविष्य कहनेवाला पुलिसिंग और बायोमेट्रिक सिस्टम हावी हो जाएंगे, जिसमें OECD के प्रवचन निगरानी को अधिनायकवादी के रूप में देखने से हटकर "स्मार्ट" शासन, स्वास्थ्य और अनुकूलन के लिए एक उपकरण के रूप में देखने की ओर स्थानांतरित हो गए हैं।

यह विकास तकनीकी नियतिवाद को दर्शाता है: प्रतिक्रियाशील अवलोकन से सक्रिय प्रोफाइलिंग तक। फिर भी, यह नैतिक चिंताएँ पैदा करता है–बड़े पैमाने पर निगरानी नियंत्रण को सामान्य बनाती है, जो पक्षपाती एल्गोरिदम के माध्यम से कमज़ोर समूहों को असमान रूप से प्रभावित करती है। ऐतिहासिक मिसालें, जैसे अमेरिकी औद्योगिक-युग की ट्रैकिंग, सत्ता के असंतुलन में निरंतरता को रेखांकित करती हैं। जैसे-जैसे AI क्षमताएँ बढ़ाता है, मानवाधिकारों के खतरों को कम करने के लिए तत्काल विनियमन की आवश्यकता है, यह सुनिश्चित करते हुए कि निगरानी समाज को अधीन किए बिना उसकी सेवा करे। (शब्द गणना: 398)

ii. भारतीय संविधान के तहत निजता के अधिकार की प्रकृति और दायरा

भारत में निजता का अधिकार, जिसे एक मौलिक अधिकार के रूप में स्थापित किया गया है, अनुचित हस्तक्षेपों के खिलाफ व्यक्तिगत स्वायत्तता, गरिमा और सूचनात्मक अखंडता की सुरक्षा को दर्शाता है। इसकी प्रकृति मानवीय गरिमा के लिए आंतरिक है, यह सुनिश्चित करती है कि व्यक्ति राज्य या सामाजिक अतिचार से मुक्त होकर आत्म-निर्धारित जीवन जी सकें। जैसा कि ऐतिहासिक जस्टिस के.एस. पुट्टास्वामी बनाम भारत संघ (2017) मामले में कहा गया है, निजता पूर्ण नहीं है, बल्कि "मानवीय गरिमा का एक तत्व" है, जो "मानव व्यक्तित्व के आंतरिक रहस्यों" को हस्तक्षेप से बचाता है। यह संविधान के अनुच्छेद 14 (समानता), 19 (भाषण, सभा आदि की स्वतंत्रता) और 21 (जीवन और स्वतंत्रता) के साथ जुड़ा हुआ है, जो मनमानी शक्ति के खिलाफ एक मजबूत दीवार बनाता है।

इसका दायरा बहुआयामी है: निर्णयात्मक निजता (शादी या

प्रजनन जैसे विकल्पों में स्वायत्तता), स्थानिक निजता (शारीरिक और घर की पवित्रता), और सूचनात्मक निजता (व्यक्तिगत डेटा पर नियंत्रण)। पुट्टास्वामी में नौ-न्यायाधीशों की पीठ ने सर्वसम्मति से एम.पी. शर्मा (1954) और खरक सिंह (1963) जैसे पहले के फैसलों को पलट दिया, जिन्होंने निजता को मौलिक अधिकार मानने से इनकार कर दिया था, और इसे "अनुच्छेद 21 के तहत जीवन और व्यक्तिगत स्वतंत्रता के अधिकार के एक आंतरिक हिस्से के रूप में संरक्षित" के रूप में पुष्टि की। यह गोबिंद बनाम मध्य प्रदेश राज्य (1975) में अनुच्छेद 21 के भीतर निजता की मान्यता से विकसित हुआ, जो अमेरिकी ग्रिसवॉल्ड बनाम कनेक्टिकट (1965) और मानवाधिकारों पर यूरोपीय कन्वेंशन जैसे वैश्विक न्यायशास्त्र से प्रभावित था।

पुट्टास्वामी के बाद, आनुपातिकता परीक्षण के माध्यम से दायरा बढ़ा: कोई भी उल्लंघन वैध होना चाहिए, एक वैध लक्ष्य (जैसे, सुरक्षा) का पीछा करना चाहिए, आवश्यक होना चाहिए (सबसे कम प्रतिबंधात्मक साधन), और आनुपातिक होना चाहिए (नुकसान को संतुलित करना)। पुट्टास्वामी II (2018) में, आधार की संवैधानिकता को बरकरार रखते हुए, न्यायालय ने स्वैच्छिक डेटा साझाकरण और दुरुपयोग के खिलाफ सुरक्षा उपायों पर जोर दिया, कल्याणकारी संदर्भों में "स्वैच्छिक" को जबरदस्ती के रूप में खारिज कर दिया। प्राइवेसी "एलिटिस्ट" नहीं बल्कि यूनिवर्सल है, जो हॉरिजॉन्टल एप्लीकेशन के ज़रिए नॉन-स्टेट एक्टर्स तक फैली हुई है।

चुनौतियाँ बनी हुई हैं: IT एक्ट (2000) जैसे कानूनों में "राष्ट्रीय सुरक्षा" के लिए अस्पष्ट छूट से ज़्यादा दखल का खतरा है। अंतरराष्ट्रीय स्तर पर, ICCPR अनुच्छेद 17 के तहत भारत की प्रतिबद्धताएँ मनमानी दखलअंदाज़ी को रोकती हैं। डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट (2023) सुरक्षा को संहिताबद्ध करता है लेकिन राज्य के लिए व्यापक छूट देता है, जो संवैधानिक सीमाओं की परीक्षा लेता है। न्यायिक विकास, ADM जबलपुर (1976) निलंबन से लेकर पुट्टास्वामी की बहाली तक, गोपनीयता के लचीलेपन को रेखांकित करता है। आखिरकार, इसका दायरा डिजिटल युग में क्षरण को रोकने के लिए मजबूत डेटा व्यवस्था, न्यायिक निगरानी और सार्वजनिक जागरूकता की मांग करता है, जिससे एक गरिमापूर्ण, न्यायसंगत समाज को बढ़ावा मिले।

iii. राष्ट्रीय सुरक्षा के संदर्भ में राज्य द्वारा डिजिटल निगरानी की आवश्यकता और औचित्य

भारतीय राज्य द्वारा डिजिटल निगरानी मुख्य रूप से राष्ट्रीय सुरक्षा की रक्षा करने, आतंकवाद, साइबर-हमलों और एक हाइपर-कनेक्टेड दुनिया में विद्रोह जैसे खतरों का मुकाबला करने के लिए एक उपकरण के रूप में उचित है। IT एक्ट (2000) की धारा 69 के तहत, यदि संप्रभुता, अखंडता, या सार्वजनिक व्यवस्था के लिए "आवश्यक या समीचीन" हो तो अवरोधन की अनुमति है - टेलीग्राफ एक्ट की "सार्वजनिक आपातकाल" की आवश्यकता से सीमाएँ कम की गई हैं। समर्थकों का तर्क है कि यह सक्रिय खुफिया जानकारी को सक्षम बनाता है: वास्तविक समय डेटा एनालिटिक्स हमलों को रोकते हैं, जैसा कि मेटाडेटा ट्रैकिंग के माध्यम से साजिशों को विफल करने में देखा गया है। 26/11 मुंबई हमलों के बाद, सेंट्रल मॉनिटरिंग सिस्टम (CMS) जैसे उपकरणों ने निगरानी को केंद्रीकृत किया, जिससे खंडित एजेंसियों की तुलना में दक्षता बढ़ी।

आवश्यकता असममित खतरों से उत्पन्न होती है - गैर-राज्य अभिनेता डिजिटल गुमनामी का फायदा उठाते हैं, जिससे पैटर्न के लिए बड़े पैमाने पर डेटा संग्रह की आवश्यकता होती है। पुट्टास्वामी फैसले (2017) ने आनुपातिकता के तहत इसका समर्थन किया: निगरानी कानूनी, वैध (सुरक्षा उद्देश्य), आवश्यक (कोई कम दखल देने वाले विकल्प नहीं), और संतुलित होनी चाहिए। भारत का भू-राजनीतिक संदर्भ - सीमा तनाव, चीन जैसे राज्य अभिनेताओं से साइबर जासूसी - तात्कालिकता को बढ़ाता है। 2023 डेटा संरक्षण अधिनियम (DPDPA) सुरक्षा के लिए राज्य के उपकरणों को छूट देता है, जो अमेरिकी FISA (1978) जैसे वैश्विक मानदंडों को दर्शाता है, जहाँ निगरानी ने 2015 पेरिस हमलों जैसी साजिशों को विफल किया।

औचित्य उपयोगितावादी नैतिकता पर आधारित है: जब

जोखिम अस्तित्वगत होते हैं तो सामूहिक सुरक्षा व्यक्तिगत गोपनीयता से अधिक महत्वपूर्ण होती है। लागत-प्रभावशीलता महत्वपूर्ण है - CCTV में चेहरे की पहचान जैसे AI-संचालित उपकरण जनशक्ति की जरूरतों को कम करते हैं, जिससे संसाधन-संकटग्रस्त बलों को मदद मिलती है। अनुभवजन्य सबूत: पेगासस जैसा स्पाइवेयर, हालांकि विवादास्पद है, लेकिन कथित तौर पर आतंकवाद की फंडिंग को बाधित करता है। OECD की चर्चाएँ निगरानी को "स्मार्ट" सुरक्षा को सक्षम बनाने के रूप में देखती हैं, जो एकीकृत शासन के लिए भारत की डिजिटल इंडिया पहल के अनुरूप है।

आलोचक इसका विरोध करते हैं कि "आवश्यकता" व्यक्तिपरक है; "सार्वजनिक व्यवस्था" जैसे अस्पष्ट शब्द असहमति के खिलाफ दुरुपयोग को सक्षम बनाते हैं, जैसा कि पेगासस द्वारा पत्रकारों को निशाना बनाने में हुआ। स्नोडेन के बाद, "अलोकतांत्रिक बदलाव" बिना सुरक्षा उपायों के बड़े पैमाने पर निगरानी को सामान्य बनाने की चेतावनी देता है। भारत में, थोक इंटरसेप्शन के लिए न्यायिक वारंट की कमी पुट्टास्वामी के आवश्यकता सिद्धांत का उल्लंघन करती है - बड़े पैमाने पर निगरानी के बजाय लक्षित निगरानी बेहतर है।

संतुलन के लिए पारदर्शिता की आवश्यकता है: वार्षिक रिपोर्ट, जैसा कि IT नियमों (2021) द्वारा अनिवार्य है, लेकिन प्रवर्तन में देरी हो रही है। अंतर्राष्ट्रीय मानक, जैसे कि EU का ई-प्राइवेसी विनियमन, न्यूनतम डेटा प्रतिधारण को अनिवार्य करते हैं। अंततः, औचित्य तभी मान्य होता है जब वह निगरानी से जुड़ा हो - सुरक्षा के लिए निगरानी अपरिहार्य है, लेकिन सत्तावादी प्रवृत्ति को रोकने के लिए जवाबदेही की आवश्यकता है, यह सुनिश्चित करते हुए कि यह लोकतंत्र की रक्षा करे न कि उसे कमजोर करे।

iv.. नागरिक स्वतंत्रता पर डिजिटल निगरानी का प्रभाव

डिजिटल निगरानी नागरिक स्वतंत्रता को गहराई से खत्म करती है, निगरानी वाले राज्य में गोपनीयता को एक ढाल से कमज़ोरी में बदल देती है। इसके मूल में, यह स्वतंत्र अभिव्यक्ति, जुड़ाव और सोच को दबाती है - जो भारतीय संविधान के अनुच्छेद 19 और 21 के लिए मुख्य हैं। जैसा कि पुट्टास्वामी (2017) ने पुष्टि की, व्यापक निगरानी सूचनात्मक गोपनीयता पर हमला करती है, एक "पैनोप्टिकॉन" बनाती है जहाँ आत्म-सेंसरशिप हावी होती है: व्यक्ति IT अधिनियम के प्रावधानों के तहत मेटाडेटा ट्रैकिंग के डर से असहमति वाले पोस्ट करने से बचते हैं। विश्व स्तर पर, ACLU की रिपोर्टें बताती हैं कि NSA के PRISM ने कैसे सक्रियता को दबाया, जो भारत के CMS की तरह है जो बिना वारंट के बड़े पैमाने पर इंटरसेप्शन की अनुमति देता है।

इसका प्रभाव कई स्तरों पर पड़ता है: समानता (अनुच्छेद 14) पर, चेहरे की पहचान जैसी पक्षपाती AI अल्पसंख्यकों की गलत पहचान करती है, जिससे नस्लीय प्रोफाइलिंग बढ़ जाती है - अमेरिकी अध्ययन गहरे रंग की त्वचा के लिए 35% तक त्रुटि दर दिखाते हैं, जिससे भारत में गलत गिरफ्तारी का खतरा होता है। जुड़ाव की स्वतंत्रता प्रभावित होती है क्योंकि सोशल ग्राफ़ नेटवर्क का खुलासा करते हैं, जिससे कार्यकर्ताओं को निशाना बनाया जाता है; 2021 में पत्रकारों के खिलाफ पेगासस स्पाइवेयर के इस्तेमाल ने राज्य की ज्यादतियों की जांच को खामोश कर दिया। बायोमेट्रिक्स के माध्यम से शारीरिक स्वायत्तता खत्म होती है - आधार को अनिवार्य रूप से लिंक करना, जिसे पुट्टास्वामी II (2018) में बरकरार रखा गया था, डेटा उल्लंघन का जोखिम पैदा करता है जिससे पहचान की चोरी या सेवाओं से बहिष्कार हो सकता है।

व्यापक नुकसान में शक्ति असंतुलन शामिल है: निगरानी जबरदस्ती, ब्लैकमेल और चयनात्मक प्रवर्तन को सक्षम बनाती है, जैसा कि अमेरिकी कारपेंटर बनाम यूनाइटेड स्टेट्स (2018) में बिना वारंट के स्थान डेटा को असंवैधानिक माना गया। भारत में, DPDPA (2023) में "सुरक्षा" के लिए छूट इसे बढ़ाती है, जिससे राज्य को बिना रोक-टोक के पहुंच मिलती है, जिससे अविश्वास और लोकतांत्रिक गिरावट को बढ़ावा मिलता है। पॉसनर जैसे आर्थिक आलोचक ध्यान देते हैं कि डेटा का व्यावसायीकरण गरिमा को खत्म करता है, जबकि नारीवादी दृष्टिकोण सार्वजनिक स्थानों पर लिंग आधारित निगरानी पर प्रकाश डालते हैं।

मनोवैज्ञानिक रूप से, लगातार निगरानी चिंता पैदा करती है,

जैसा कि हार्वर्ड लॉ रिव्यू के विश्लेषण बताते हैं, जिससे नवाचार और नागरिक जुड़ाव बाधित होता है। कमजोर समूह - अल्पसंख्यक, LGBTQ+ - बढ़े हुए जोखिमों का सामना करते हैं; संयुक्त राष्ट्र की रिपोर्टों के अनुसार, स्पाइवेयर फोन को "24 घंटे के जासूस" में बदल देता है, जिससे अंतरंगता का हथियार के रूप में इस्तेमाल होता है।

फिर भी, बचाव के तरीके मौजूद हैं: एन्क्रिप्शन इंटरसेप्शन से बचाता है, और न्यायिक वारंट जैसी निगरानी दुरुपयोग को रोकती है। भारत की यात्रा, खड़क सिंह (1963) के घर-घर जाकर निगरानी से लेकर आधुनिक डेटा निगरानी तक, तात्कालिकता को रेखांकित करती है। सुधार के बिना, निगरानी सुरक्षा नहीं बढ़ाती बल्कि समुदायों को अलग-थलग करती है, जैसा कि ब्रेनन सेंटर की फाइंडिंग्स से पता चलता है–प्रोफाइलिंग विश्वास को खत्म करती है, जिससे इंटेलिजेंस में बाधा आती है। आखिरकार, इसका अनियंत्रित विस्तार स्वतंत्रता-सुरक्षा संतुलन को खतरे में डालता है, जिसके लिए नागरिक समाज की जीवंतता को बनाए रखने के लिए अधिकारों पर आधारित रीकैलिब्रेशन की आवश्यकता है।

v. राष्ट्रीय सुरक्षा और निजता के अधिकार के बीच संतुलन बनाने के लिए कानूनी और नीतिगत उपाय

भारत में राष्ट्रीय सुरक्षा और निजता के बीच संतुलन बनाने के लिए पुट्टास्वामी (2017) के आनुपातिकता परीक्षण पर आधारित एक बहुआयामी ढांचे की आवश्यकता है: वैधता, वैध उद्देश्य, आवश्यकता और न्यूनतम हस्तक्षेप। कानूनी तौर पर, सभी निगरानी के लिए न्यायिक वारंट अनिवार्य करने के लिए IT अधिनियम (2000) में संशोधन करें, कार्यकारी "संतुष्टि" को पूर्वव्यापी निगरानी से बदलें, जैसा कि अमेरिकी FISA अदालतों में होता है। एक निगरानी आयुक्त नियुक्त करें, जो कार्यपालिका से स्वतंत्र हो, जो सालाना प्राधिकरणों की समीक्षा करे, और अवर्गीकृत रिपोर्टों के माध्यम से पारदर्शिता सुनिश्चित करे–जो UK के इन्वेस्टिगेटरी पावर्स एक्ट (2016) के समान हो।

DPDPA (2023) को मजबूत किया जाना चाहिए: धारा 17 की छूट को "अत्यावश्यक सामाजिक जरूरतों" तक सीमित करें, और राज्य को व्यापक छूट देने पर रोक लगाएं। डेटा मिनिमाइजेशन लागू करें–केवल परिभाषित अवधियों के लिए आवश्यक मेटाडेटा बनाए रखें (जैसे, अधिकतम 2 साल)–और एक्सेस लॉग के लिए ऑडिट ट्रेल्स रखें। नीतिगत रूप से, बिना डिक्रिप्शन के सुरक्षित विश्लेषण के लिए होमोमोर्फिक एन्क्रिप्शन जैसी गोपनीयता बढ़ाने वाली तकनीकों (PETs) को अपनाएं, जिससे उल्लंघन का जोखिम कम हो। EU GDPR के अनुसार, निगरानी उपकरणों के लिए प्रभाव आकलन अनिवार्य करें, जिसमें पूर्वाग्रहों और विकल्पों का मूल्यांकन किया जाए।

स्वतंत्र निकाय, जैसे कि जांच शक्तियों वाला एक डेटा संरक्षण प्राधिकरण, अनुपालन की निगरानी करे, और उल्लंघन के लिए टर्नओवर के 4% तक का जुर्माना लगाए। सार्वजनिक भागीदारी महत्वपूर्ण है: दुर्व्यवहार की रिपोर्ट करने के लिए नागरिक निगरानी पैनल और व्हिसलब्लोअर सुरक्षा स्थापित करें, जिससे विश्वास बढ़े। अंतरराष्ट्रीय स्तर पर, सीमा पार डेटा साझाकरण को सीमित करने वाले द्विपक्षीय समझौतों के माध्यम से ICCPR अनुच्छेद 17 के साथ तालमेल बिठाएं।

न्यायिक रूप से, पुट्टास्वामी II (2018) के सिद्धांतों का विस्तार करें ताकि आनुपातिकता के बिना पेगासस जैसे असंगत उपायों को रद्द किया जा सके। विधायी सुधारों में एक व्यापक गोपनीयता अधिनियम शामिल है जो निगरानी नियमों को एकीकृत करता है, जिसमें आपातकालीन शक्तियों के लिए सनसेट क्लॉज शामिल हैं।

वैश्विक मॉडलों से मिले सबूत–कनाडा के चार्टर-अनिवार्य समीक्षाओं ने अत्यधिक हस्तक्षेप को कम किया–बताते हैं कि ये उपाय दुरुपयोग को रोकते हैं जबकि सुरक्षा को सक्षम बनाते हैं। भारत में, 2021 के पेगासस कांड के बाद, ऐसे उपाय असहमति के दमन को रोक सकते हैं। आखिरकार, संतुलन के लिए गोपनीयता को सुरक्षा के प्रवर्तक के रूप में देखने की आवश्यकता है: ब्रुकिंग्स के विश्लेषण के अनुसार, अलग-थलग नागरिक जानकारी नहीं देते हैं। मज़बूत कानूनों, टेक सुरक्षा उपायों और जवाबदेही के ज़रिए, भारत संवैधानिक मूल्यों को दांव पर लगाए बिना सर्विलांस के फायदों का

इस्तेमाल कर सकता है, और एक मज़बूत लोकतंत्र को बढ़ावा दे सकता है।

7. सरकारी निगरानी कार्यक्रमों के लिए निगरानी तंत्र

सरकारी निगरानी की देखरेख आमतौर पर न्यायिक, विधायी और स्वतंत्र तरीकों के मिश्रण से की जाती है, लेकिन उनकी ताकत और स्वतंत्रता हर देश में अलग-अलग होती है। मज़बूत निगरानी के लिए स्पष्ट कानूनी शक्तियों, गोपनीय जानकारी तक पहुंच और बाध्यकारी निष्कर्ष या समाधान जारी करने की क्षमता की ज़रूरत होती है, जिसकी कमी अभी भी कई सिस्टम में है।

न्यायिक निगरानी: न्यायिक तरीकों में आमतौर पर अदालतें या विशेष जज शामिल होते हैं जिन्हें पहले से ही दखल देने वाले निगरानी उपायों, जैसे कि वायरटैप या संचार को इंटरसेप्ट करने की अनुमति देनी होती है। कुछ देशों में, विशेष अदालतें या पैनल (उदाहरण के लिए, ऐसे निकाय जो खुफिया तरीकों को मंज़ूरी दे सकते हैं या मना कर सकते हैं और बाद में शिकायतों की समीक्षा कर सकते हैं) बाध्यकारी फैसले देते हैं जो खुफिया एजेंसियों को सीमित करते हैं।

संसदीय और कार्यकारी निगरानी: विधानमंडल अक्सर खुफिया या सुरक्षा समितियां बनाते हैं जो एजेंसियों के बजट, जनादेश और कानून के पालन की समीक्षा करती हैं, और अधिकारियों को गवाही देने के लिए बुला सकती हैं या दस्तावेज़ मांग सकती हैं। कार्यकारी शाखा के निकाय, जैसे कि आंतरिक महानिरीक्षक या सलाहकार बोर्ड, निगरानी अभियानों की वैधता और प्रभावशीलता की निगरानी करते हैं और सरकार के प्रमुखों या संबंधित मंत्रियों को रिपोर्ट करते हैं।

स्वतंत्र पर्यवेक्षी निकाय: कई लोकतंत्रों में स्वतंत्र निगरानी संस्थान होते हैं जैसे कि खुफिया लोकपाल, डेटा संरक्षण प्राधिकरण, या विशेष समीक्षा एजेंसियां जिनके पास गोपनीय सामग्री तक व्यापक पहुंच होती है। ये निकाय निरीक्षण कर सकते हैं, नागरिकों की शिकायतों की जांच कर सकते हैं, सार्वजनिक रिपोर्ट प्रकाशित कर सकते हैं, और कुछ सिस्टम में गैर-कानूनी तरीकों को रोकने या डेटा हैंडलिंग को ठीक करने के लिए बाध्यकारी आदेश जारी कर सकते हैं।

आंतरिक नियंत्रण और पारदर्शिता उपकरण: एजेंसियों के भीतर, आंतरिक अनुपालन इकाइयों, ऑडिट लॉग और प्राधिकरण श्रृंखलाओं का उपयोग यह जांचने के लिए किया जाता है कि निगरानी शक्तियों का उपयोग कानूनी रूप से और केवल अधिकृत कर्मियों द्वारा किया जा रहा है या नहीं। बाहरी पारदर्शिता उपायों, जैसे कि इंटरसेप्शन शक्तियों के उपयोग पर समय-समय पर सार्वजनिक रिपोर्टिंग और निगरानी कानूनों की अनिवार्य विधायी समीक्षा, कार्यक्रमों को आवश्यकता और आनुपातिकता मानकों के अनुरूप रखने के लिए तेजी से सिफारिश की जा रही है।

उदाहरण: भारत में सीमित निगरानी: भारत में, टेलीग्राफ अधिनियम और सूचना प्रौद्योगिकी अधिनियम के तहत संचार को इंटरसेप्ट करने की निगरानी मुख्य रूप से अदालतों या संसद के बजाय वरिष्ठ नौकरशाहों की एक कार्यकारी समीक्षा समिति द्वारा की जाती है। हाल के विश्लेषणों से पता चलता है कि खुफिया एजेंसियों की अभी भी कोई व्यापक, स्वतंत्र या संसदीय निगरानी नहीं है, और न्यायिक या स्वतंत्र समीक्षा को अधिक अधिकार-सुरक्षात्मक विकल्प के रूप में पेश करने के लिए सुधारों पर ज़ोर दिया गया है।

8. अंतर्राष्ट्रीय संधियाँ और सीमा पार निगरानी

अंतर्राष्ट्रीय संधियाँ मुख्य रूप से सीमाओं से परे गोपनीयता सुरक्षा का विस्तार करके, आवश्यकता और आनुपातिकता की मांग करके, और यह विनियमित करके कि राज्य दूसरे देशों में संग्रहीत डेटा तक कैसे पहुँच सकते हैं, सीमा पार निगरानी को प्रतिबंधित करती हैं। वे सभी विदेशी खुफिया जानकारी इकट्ठा करने पर प्रतिबंध नहीं लगाती हैं, लेकिन वे इसे मानवाधिकार दायित्वों, क्षेत्राधिकार नियमों और विशेष साइबर अपराध सहयोग ढाँचों के माध्यम से सीमित करती हैं।

मानवाधिकार संधियाँ और क्षेत्राधिकार: इंटरनेशनल कोवेनेंट ऑन सिविल एंड पॉलिटिकल राइट्स (ICCPR) और यूरोपियन कन्वेंशन ऑन ह्यूमन राइट्स (ECHR) जैसी संधियाँ गोपनीयता और पत्राचार की रक्षा करती हैं, और तेजी से यह व्याख्या की जा रही है कि जब कोई राज्य अपने क्षेत्र के बाहर लेकिन अपने "अधिकार क्षेत्र" के भीतर लोगों की

निगरानी करता है (उदाहरण के लिए, जब उनके संचार को इंटरसेप्ट करता है) तो ये लागू होती हैं। विशेषज्ञ सिद्धांत और केस कानून इस बात पर जोर देते हैं कि ऐसी विदेशी निगरानी को घरेलू निगरानी के समान वैधता, वैध उद्देश्य, आवश्यकता और आनुपातिकता के परीक्षणों को पूरा करना चाहिए, और इसमें दुरुपयोग के खिलाफ सुरक्षा उपाय शामिल होने चाहिए।

सामूहिक विदेशी इंटरसेप्शन पर क्षेत्रीय न्यायालय की सीमाएँ: यूरोपियन कोर्ट ऑफ ह्यूमन राइट्स ने स्वीकार किया है कि राज्य विदेशी-केंद्रित इंटरसेप्शन सिस्टम चला सकते हैं, लेकिन केवल स्पष्ट कानूनों के तहत जो सख्ती से परिभाषित करते हैं कि किस सीमा पार ट्रैफिक को इंटरसेप्ट किया जा सकता है, इसे कितने समय तक रखा जा सकता है, और कौन सी स्वतंत्र निगरानी मौजूद है। हाल के यूरोपीय निर्णयों और राष्ट्रीय न्यायालयों के फैसलों ने सीमा पार संचार के सामूहिक इंटरसेप्शन पर सवाल उठाया है या प्रतिबंधित किया है जहाँ सुरक्षा उपाय अपर्याप्त हैं, और गोपनीयता और डेटा सुरक्षा के मौलिक अधिकारों के साथ असंगति पाई है।

साइबर अपराध संधियाँ और डेटा एक्सेस: बुडापेस्ट कन्वेंशन ऑन साइबरक्राइम और इसके अनुवर्ती उपकरण संग्रहीत कंप्यूटर डेटा तक सीमा पार पहुँच के लिए एक ढाँचा बनाते हैं, जिसमें आम तौर पर एकतरफा गुप्त पहुँच के बजाय पारस्परिक कानूनी सहायता या अन्य औपचारिक सहयोग चैनलों की आवश्यकता होती है। अनुच्छेद 32 सीमित एकतरफा पहुँच की अनुमति केवल तभी देता है जब डेटा सार्वजनिक रूप से उपलब्ध हो या जब विदेशी डेटा धारक सहमति दे, जो अप्रत्यक्ष रूप से राज्यों को सहमत प्रक्रियाओं के बजाय गुप्त सीमा पार निगरानी का उपयोग करने से रोकता है।

संयुक्त और साझा निगरानी के लिए जिम्मेदारी: अंतर्राष्ट्रीय मानवाधिकार कानून सीमा पार खुफिया जानकारी साझा करने को भी सीमित करता है, यह सुझाव देता है कि यदि कोई राज्य ऐसी योजनाओं में भाग लेता है जो विदेश में गोपनीयता या अन्य अधिकारों का उल्लंघन करती हैं, तो वह जिम्मेदारी ले सकता है, भले ही कोई दूसरा राज्य तकनीकी इंटरसेप्शन सिस्टम संचालित करता हो। यह राज्यों को यह सुनिश्चित करने के लिए प्रेरित करता है कि सूचना-साझाकरण समझौते, संयुक्त डेटाबेस और सहकारी इंटरसेप्शन कार्यक्रमों में उनकी संधि दायित्वों के अनुरूप सुरक्षा उपाय शामिल हों।

व्यावहारिक सीमाएँ और कमियाँ: इन प्रतिबंधों के बावजूद, महत्वपूर्ण कमियाँ बनी हुई हैं क्योंकि कई संधियों में स्पष्ट निगरानी नियमों की कमी है, प्रवर्तन धीमा है, और शक्तिशाली राज्य गोपनीयता अधिकारों के क्षेत्राधिकार से बाहर आवेदन पर विवाद करते हैं। नतीजतन, अभी ज़्यादातर क्रॉस-बॉर्डर सर्विलांस को डिजिटल इंटेलिजेंस एक्टिविटीज़ के लिए खास तौर पर बनाए गए, विस्तृत, बाध्यकारी संधि प्रावधानों के बजाय, विकसित हो रहे कोर्ट के फैसलों, एक्सपर्ट गाइडलाइंस और सॉफ्ट-लॉ स्टैंडर्ड्स से ज़्यादा चेक किया जाता है।

9. सुझाव (Suggestions)

डिजिटल निगरानी और निजता के अधिकार के बीच संतुलन स्थापित करने के लिए निम्नलिखित सुझाव दिए जाते हैं:

1. निगरानी से संबंधित कानूनों में स्पष्टता और पारदर्शिता सुनिश्चित की जाए।
2. स्वतंत्र निगरानी और जवाबदेही तंत्र की स्थापना की जाए।
3. डेटा न्यूनतमकरण और उद्देश्य-सीमित उपयोग के सिद्धांतों को अपनाया जाए।
4. नागरिकों को उनके डेटा अधिकारों के प्रति जागरूक किया जाए।
5. अंतरराष्ट्रीय सर्वोत्तम प्रथाओं को भारतीय संदर्भ में अपनाया जाए।

10. निष्कर्ष (Conclusion)

डिजिटल निगरानी आधुनिक शासन का एक अपरिहार्य अंग बन चुकी है, विशेष रूप से राष्ट्रीय सुरक्षा के संदर्भ में। किंतु एक लोकतांत्रिक समाज में सुरक्षा और स्वतंत्रता को परस्पर विरोधी नहीं, बल्कि पूरक के रूप में देखा जाना चाहिए। निजता का अधिकार व्यक्ति की गरिमा और स्वतंत्रता का आधार है। यदि राज्य द्वारा निगरानी बिना पर्याप्त विधिक सुरक्षा के की जाती है, तो यह लोकतंत्र की जड़ों को कमजोर

कर सकती है। इसलिए आवश्यक है कि निगरानी को संवैधानिक सीमाओं में रखते हुए, पारदर्शी और जवाबदेह बनाया जाए। अंततः, राष्ट्रीय सुरक्षा और नागरिक स्वतंत्रताओं के मध्य संतुलन ही एक सशक्त और न्यायसंगत डिजिटल समाज की आधारशिला हो सकता है।

संदर्भ (References)

1. Sharma, S. (2021). डिजिटल युग में निजता का अधिकार. नई दिल्ली: यूनिवर्सल लॉ पब्लिशिंग।
2. Verma, R. (2020). राष्ट्रीय सुरक्षा बनाम नागरिक स्वतंत्रता: डिजिटल निगरानी की भूमिका. भारतीय विधि समीक्षा, 12(2), 45-60।
3. Singh, P. (2019). सूचना प्रौद्योगिकी कानून और निजता. लखनऊ: ईस्टर्न बुक कंपनी।
4. Gupta, A. (2022). डिजिटल निगरानी और संविधान का अनुच्छेद 21. संविधानिक अध्ययन पत्रिका, 8(1), 78-92।
5. Mishra, K. (2021). साइबर कानून और मानवाधिकार. भोपाल: मध्य प्रदेश हिंदी ग्रंथ अकादमी।
6. Yadav, N. (2020). भारत में राज्य निगरानी और नागरिक अधिकार. समकालीन विधि जर्नल, 5(3), 110-125।
7. Pandey, S. (2018). सूचना का अधिकार एवं निजता. इलाहाबाद: लॉ पब्लिशर्स (इंडिया)।
8. Tiwari, M. (2023). डिजिटल इंडिया और निजता की चुनौतियाँ. भारतीय सामाजिक विज्ञान पत्रिका, 15(2), 134-148।
9. Saxena, D. (2022). राष्ट्रीय सुरक्षा कानून और डिजिटल तकनीक. जयपुर: राज पब्लिशर्स।
10. Chaudhary, R. (2019). निगरानी राज्य की अवधारणा और लोकतंत्र. लोकतंत्र एवं विधि, 6(1), 55-70।
11. Solove, D. J. (2008). Understanding privacy. Harvard University Press.
12. Greenleaf, G. (2014). Global data privacy laws: 89 countries, and accelerating. Privacy Laws & Business International Report, 115, 1-6.
13. Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.
14. Kuner, C. (2017). Transborder data flows and data privacy law. Oxford University Press.
15. Richards, N. M. (2013). The dangers of surveillance. Harvard Law Review, 126(7), 1934-1965.
16. K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
17. Information Technology Act, 2000 (India).
18. Digital Personal Data Protection Act, 2023 (India).
19. European Union. (2016). General Data Protection Regulation (GDPR).
20. United Nations. (1948). Universal Declaration of Human Rights.
21. Constitution of India.

Feedback Form

Your valuable comments will help us to shape the future issues better.

	Highly Appreciable	Somewhat Appreciable	Not Appreciable	Did Not Read
The Impact Of Cybersecurity And Data Protection Regulations On Startup Innovation And Performance: Evidence From Emerging Economies	☐	☐	☐	☐
The Role Of Patent Law In Promoting Pharmaceutical Innovation: Ethical And Regulatory Perspectives	☐	☐	☐	☐
Tech-driven Solutions To Global Death Penalty Challenges: Legislative And Judicial Approaches To Mandatory Capital Punishment In India And The USA	☐	☐	☐	☐
Regulating Online Platform: Impact Of Online Harassment And Hate Speech On Women Participation In Political Activities	☐	☐	☐	☐
How AI Tools Challenge Traditional Methods Of Legal Interpretation: A Comparative Analysis With Indian Context	☐	☐	☐	☐
Re-Imagining Copyright Governance In India: Legal And Ethical Challenges In The Age Of Artificial Intelligence	☐	☐	☐	☐
Balancing Privacy And Public Interest: The Emerging Landscape Of The Right To Be Forgotten In India	☐	☐	☐	☐
Guardians Of Data: From Brussels To Bharat	☐	☐	☐	☐
The Commons That Feed The Machines: Policy Reflections On Ai's Use Of Public Domain Works	☐	☐	☐	☐
Regulating Lantana Camara: A Legal Analysis With Special Reference To Deepor Beel In Assam	☐	☐	☐	☐
The Role Of AI Arti ficial Intelligence In The Consumer Protection Act of 2019	☐	☐	☐	☐
Migration-related Vulnerabilities And Legal Safeguards For Women In Jammu & Kashmir	☐	☐	☐	☐
डिजिटल निगरानी और निजता का अधिकार: राष्ट्रीय सुरक्षा एवं नागरिक स्वतंत्रताओं का संतुलन	☐	☐	☐	☐

Comments/Suggestions (if any) : .....

.....

Name :Mr/Ms. .....

Designation : .....Organization / Institution : .....

Address : .....

Phone : .....

E-mail : .....E-mail : .....

Subscription Form

I wish to subscribe to /renew my subscription to IPEM Law Journal for 1/2/3 year(s). A bank draft / cheque bearing no ..... dated ..... for Rs. ..... drawn in favour of **IPEM LAW ACADEMY** payable at GHAZIABAD/DELHI towards subscription for years, is enclosed.

Subscription Rate Details

Category	INDIA		ASIAN COUNTERIES		OTHER COUNTERIES	
Duration	Individual	Institutional	Individual	Institutional	Individual	Institutional
1 Year	750	1000	80	85	100	150
2 Year	1250	1750	170	175	200	300
3 Year	1800	2300	220	225	250	350
Lifetime	6500	8500	1000	1100	1400	1800

The Chief Editor

IPEM LAW JOURNAL

Institute of Professional Excellence & Management

A-13/1, S.S. G.T. Road, Industrial Area, NH-24 Bypass

Ghaziabad-201010

Tel. : 0120-4174500

Affix Postal Stamp

The Chief Editor

IPEM LAW JOURNAL

Institute of Professional Excellence & Management

A-13/1, S.S. G.T. Road, Industrial Area, NH-24 Bypass

Ghaziabad-201010

Tel. : 0120-4174500

Affix Postal Stamp