



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]



Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

“Law in the Age of Artificial Intelligence: A Fundamental Perspective”

Organised by KES’ Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: <https://doi.org/10.70183/lijdlr.2026.v4si1.15>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE

About the College



KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

KANDIVLI EDUCATION SOCIETY

Established 1936



Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

EDUCATIONAL COMMITMENT

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

LAW IN THE AGE OF ARTIFICIAL INTELLIGENCE

A Fundamental Perspective



ABOUT THE INTERNATIONAL CONFERENCE

The International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective” provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

PRINCIPAL'S MESSAGE

KES' Shri. Jayantilal H. Patel Law College



It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective.”

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

DR. VIRAL DAVE

I/c. Principal

KES' Shri. Jayantilal H. Patel Law College

ORGANISING COMMITTEE

International Conference on Law in the Age of Artificial Intelligence



I/c. Principal

Dr. Viral Dave

Convenor

Mr. Mahavir Mandot

Co-Convenors

Dr. Shweta Vijendra Pathak

Ms. Priyanka Khakhadia

Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

*Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of
Doctrinal Legal Research [Volume IV, Special Issue I, 2026]*

CRIMINAL ATTRIBUTES EMERGING FROM CRIME MAPPING: A HUMAN RIGHTS PERSPECTIVE

Sri Meena S¹

I. ABSTRACT

In the 21st century, the utilization of artificial intelligence (AI) on employment, public services, surveillance significantly developed the socio-economic landscape. At the International level, cases such as the Dutch child benefits scandal and the use of the crime mapping in U.S. courts reveal serious governance failures in algorithmic decision-making. In the Indian context, the deployment of the CMAPS by the Delhi Police in the Jahangirpuri area has raised significant human rights concerns. The use of facial recognition technology has contributed to disproportionate arrests of Dalits and Muslims. In further, discriminatory recruitment algorithms in industrial AI applications such as Amazon's hiring system, underscore issues of privacy violations, algorithmic bias, and unfair attribution. All these incidents are given clear picture about the violation of AI driven crime mapping in International and national human rights regime. Indian Constitution guarantees the human rights to protect the marginalized people from unfairness, discrimination, deprivation. From an ethical perspective, AI decision-making must be grounded in transparency, accountability, human dignity rather than merely technical preference. Through the analytical, multi-disciplinary, philosophical and humanitarian approaches, paper examines how AI governance must be anchored in ethical obligations and universal principles, highlights the requirement of human supervision on AI, challenges posed by AI-driven criminal attribution due to legal vacuum. Furthermore, the paper emphasizes that true development lies in restoring the public trust, safeguarding human rights and ensuring the remedial justice (ubi jus ibi remedium). Finally, the paper proposes remedial measures including technical safeguards, curriculum reform through awareness, and the formulation of strategic policy guidelines for effective governance.

¹ 4th semester B. A. L. L. B Student at government law college, Madurai (India).Email: Srimeenu777@gmail.com

II. KEYWORDS

Predictive Policing, Algorithmic Bias, Facial Recognition Technology, Human Rights, AI Governance.

III. INTRODUCTION

In the contemporary phase of technological evolution, society has entered the era of artificial intelligence. At present, various sectors such as architecture, education, programming, law, and astronomy increasingly employ AI to enhance the scope of their respective fields, facilitate efficient problem-solving, and support informed decision-making processes.

According to Marvin Minsky, AI is the science of making machines do things that would require intelligence if done by human² Understanding artificial intelligence involves recognizing it as an enabling system that integrates multiple technologies to process input data provided by individuals to perform tasks or support decision-making.

Since 2020, the rapid advances in AI, particularly towards Artificial General Intelligence (AGI) have significantly reshaped social media interactions. Individuals across all aged group from infants to senior citizens, actively engaging with generative AI to transform text into images, video and other digital content.

In governance and security bodies such as the police, the military is using AI for crime detection and hotspot mapping. The use of AI reflects a positive impact, on other hand AI-driven phishing³ attacks by cyber attackers can violate confidential areas like privacy, human rights principles, and sovereign interests.

² J D Bolter, 'Artificial Intelligence' (1984) 113(3) *Daedalus* 1 <http://www.jstor.org/stable/20024925> > accessed 16 Jan 2026.

³ Phishing is a type of social engineering attack where attackers set up a fraudulent website designed to look like a legitimate website and to lure users into putting their personal information. Such social engineering attacks currently affect billions of Internet users. W Lee, J Hur and D Kim, 'Examining Phishing Kits through Script-Level Analysis and Their Influence on Operational Phishing Websites' (2024) *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIA CCS '24)* 1 <https://doi.org/10.1145/3634737.3657013> > accessed 17 Jan 2026.

A. Research Objectives

1. The primary objective of this paper is to examine the ethical concerns from the contemporary application of AI, particularly in surveillance, risk assessment, and decision-making systems that affected marginalized people.
2. It further seeks to analyze the operation of AI-driven crime mapping and predictive policing systems within human rights frameworks.
3. The paper also evaluates the impact of algorithmic bias on vulnerable communities to assess the adequacy of existing legal remedies and to evaluate the essence of a right-based regulatory framework to uphold human centric governance.
4. To analyze the key takeaways from the international frameworks to deal with the AI crisis.

B. Research Question

1. This paper interrogates whether AI tool is merely technology advancement or instead operates as transformative force reshaping the governance?
2. Whether AI tool disproportionately impact the marginalized the vulnerable people?
3. Whether fundamental human rights principles can be effectively upheld through judicial activism, in accordance with the legal maxim *ubi jus ibi remedium* (where there is a right, there is a remedy) in the licit world?

C. Research Methodology

This paper employs a philosophical and analytical research methodology, supplemented by a limited comparative approach to provide a comprehensive analysis through Simultaneously, the analytical method is utilized to critically evaluate jurisprudential

theories including Kantian⁴ deontology and Roscoe Pound's theory of social engineering to assess the ethical foundations underpinning AI governance.

Through a multidisciplinary approach drawing on legal theory, socio-technical studies, and philosophy, the paper discusses ethical concerns arising from AI systems, including algorithmic bias, racial and religious profiling, gender-based discrimination, and nationality-based attribution of suspicion.

By adopting a case-study methodology, this paper examines how marginalised communities may be adversely affected when AI tools function not merely as instruments of human welfare, but as mechanisms capable of reinforcing structural inequalities

This paper relies on primary sources such as constitutional provisions, statutory frameworks, judicial precedents, and International human rights instruments, such as the Universal Declaration of Human Rights⁵ (UDHR) and the International Covenant on Civil and Political Rights⁶ (ICCPR). In addition, it referred to research articles, scholar opinions, policy recommendations, and committee reports.

In view of the above, the paper is structured into three parts: first, a factual analysis of AI-driven crime mapping and the operational impact of predictive algorithms; second, a jurisprudential examination of predictive policing algorithms; and third, solution-based justice mechanisms for AI-assisted crime mapping

IV. FACTUAL ANALYSIS OF AI-DRIVEN CRIME MAPPING: PREDICTIVE ALGORITHMS AND THEIR OPERATIONAL IMPACT

In exponential growth of generative AI since 2020 has been driven by high using platforms such as ChatGPT, Google Gemini, Copilot, as well as image generators Dall-E2, Elicit. The generative AI is used across various sectors such as designing, coding,

⁴Immanuel Kant (1993) [1785]. *Groundwork of the Metaphysics of Morals*. Translated by Ellington, James W. (3rd ed.). Hackett. ISBN0-87220-166-X > accessed 17 Jan 2026.

⁵ Universal Declaration of Human Rights (1948) <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. > accessed 17 Jan 2026.

⁶ International Covenant on Civil and Political Rights (adopted 19 December 1966, entered into force 23 March 1976) 999 UNTS 171, Can TS 1976 No 47 [ICCPR]. > accessed 16 Jan 2026.

writing, education, and customer service. However, generative AI also misused for cybercrime activities includes deceive, manipulate through the fake information. In International context, Northpointe developed a COMPAS (Correctional Offender Management Profiling for Alternative Sanction) tool as a risk assessment system that uses algorithms to predict an offender on such a recidivist basis of their past crime record.

Using the past periodical records of data the Predictive AI operates, anticipate the future outcomes. However, in US court system COMPAS tool is biased against African American rather than white Americans, research work of ProPublica⁷ found that Black defendants almost nearly twice as likely as White defendants to be wrongly labeled as high profile criminals, even they didn't reoffend the crime, while white defendants were more likely to be classified as low risk despite committing further crimes. In the case of *State v Loomis*⁸ 881 N.W.2d 74 the defendant, Eric Loomis, was sentenced to six years of imprisonment and five years of extended supervision, a decision influenced by a high-risk recidivism score generated by the COMPAS algorithm, the study of ProPublica⁹ reveals moreover 7000 were convicted in Broward County, Florida.

Similarly, the Dutch childcare benefits scandal¹⁰, emerged as one of the most serious, ruthless crises in modern Dutch history. The use of the System Risk Indication (SyRI), an opaque algorithmic risk-profiling system, alleged moreover 35,000 parents being wrongfully accused on childcare benefit fraud¹¹, it disproportionately targeting individuals with migrant backgrounds and dual nationality. In over 2,000 cases of

⁷ J Angwin, J Larson, S Mattu and L Kirchner, 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks' ProPublica (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> > accessed 17 Jan 2026.

⁸ *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016))

⁹ J Angwin, J Larson, S Mattu and L Kirchner, 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks' ProPublica (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> > accessed 18 Jan 2026.

¹⁰ Josien Arts and Marguerite van den Berg, 'What the Dutch benefits scandal and policy's focus on "fraud" can teach US about the endurance of empire' (2025) *Critical Social Policy* 45(1) 177-187 <https://doi.org/10.1177/02610183241281346> accessed 17 Jan 2026.

¹¹ Dienst Toeslagen, 'Toeslagen Herstel: Feiten en Cijfers' (2024) <https://herstel.toeslagen.nl/dashboard-kinderopvangtoeslag/>. > accessed 17 Jan 2026.

allegations resulted in severe consequences such as the loss of child custody¹²this underscores the crucial status of human rights posed by unregulated algorithmic governance.

In 2018, Amazon scrapped its secret AI tool¹³following controversy regarding discrimination. It shows how AI driven decision-making systematically denied opportunities to women due to male-dominated employment historical data records, violates the principle of equal opportunity and non-discrimination. It underscores the critical need for transparency, accountability, and human rights-centric frameworks.

V. JURISPRUDENTIAL EXAMINATION ON PREDICTIVE POLICING ALGORITHMS

Artificial intelligence plays a pivotal role in transforming the world, but its complexity creates serious ethical concerns between the AI and transparency, fairness, non-discrimination like hood ethical values. Ethics consist of jurisprudence concepts as branch another hand jurisprudence contains ethical principles however, these varieties own force and dignity. And, therefore, ethics influences jurisprudence more by bringing to it life and light from without, than by holding an artificial and false position within the jural sphere.¹⁴

The rapid growth of AI has created an urgent need for ethical regulation in areas such as privacy, accountability, and bias, because AI mechanisms often rely on large volumes of personal, sensitive, and confidential data

¹² Centraal Bureau voor de Statistiek (CBS), 'Kenmerken van Gedupeerde Gezinnen Toeslagenaffaire' (2022) <https://www.cbs.nl/nl-nl/maatwerk/2022/26/kenmerken-van-gedupeerde-gezinnen-toeslagenaffaire>. > accessed 17 Jan 2026.

¹³ J Dastin, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women' *Reuters* (10 October 2018) <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G> > accessed 18 Jan 2026.

¹⁴ Miss Chaturvedi, 'AI and Ethics: Jurisprudential Psychology to Investigate How Far It Can Be Regulated' (2025) 28 *American Journal of Psychiatric Rehabilitation* 784 <https://doi.org/10.69980/ajpr.v28i1.194> accessed 17 Jan 2026.

For example, in the IIT Naya Raipur around 36 girl student images are misused by Co-student using AI¹⁵ Furthermore, NCMEC's.¹⁶ CyberTipline received approximately 4,700 reports in 2023 specifically involving child sexual abuse material or sexually exploitative content linked to generative AI technology, against the broader context of more than 36.2 million CyberTipline reports received that year. In an ethical approach, AI social influence exacerbates ethical concerns such as inequality, job displacement, privacy matters, and raising questions about ethical standards of AI.

By applying Immanuel Kant's deontological ethics¹⁷, particularly in the idea on the second formulation of the categorical imperative that; "What has a price can be replaced by something else as its equivalent; what on the other hand is raised above all price and therefore admits of no equivalent has a dignity" (Groundwork 4:434) "So, act that you use humanity, whether in your own person or in the person of any other, always at the same time as an end, never merely as a means" (Groundwork 4:429)

This moral evaluation mandates strict adherence to duties and universal rules, and highlights the importance of human dignity in the current context of AI. It also requires human supervision of AI systems to prevent discrimination, wrongful criminal attribution, and deprivation of rights.

After the implementation of UDHR (1948)¹⁸, most of the nation's enshrines the fundamental rights of humans through their governance, especially police using Facial Recognition Technology" As a process or set of rules to be followed to calculate or analyses facial characteristics ... by a computer."¹⁹ Through algorithms, it collects and

¹⁵ R Drolia, 'Chhattisgarh: IIT Naya Raipur Student Held for Morphing Photos of Fellow Girls Using AI Tools' *Times of India* (9 October 2025) <https://timesofindia.indiatimes.com> accessed 18 Jan 2026.

¹⁶ National Center for Missing & Exploited Children (NCMEC), 'Generative AI CSAM is CSAM' <https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam> accessed 17 Jan 2026.

¹⁷ Immanuel Kant (1993) [1785]. *Groundwork of the Metaphysics of Morals*. Translated by Ellington, James W. (3rd ed.). Hackett. ISBN0-87220-166-X. > accessed 17 Jan 2026.

¹⁸ Universal Declaration of Human Rights (1948) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 19 Jan 2026.

¹⁹ I Berle, *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images* (Springer, Switzerland 2020) <https://doi.org/10.1007/978-3-030-36887-6> accessed 17 Jan 2026.

identifies biometrics which can be used to detect and penalize criminals. However, Vidhi Centre for Legal Policy²⁰ reported that the belief that certain communities possess an inherent “disposition toward crime” legitimizes over-policing and results in the systematic victimization of marginalized groups, particularly Muslims and Dalits.

AI-driven predictive algorithms such as COMPAS, and in the Indian context CMAPS the Crime Mapping Analytics and Predictive System are used to identify crime hotspots and assist policing. However, when such systems rely on historically biased data or parameters linked to religion, gender, caste, migration status, or community identity, they may reinforce discriminatory outcomes.²¹ Following the communal violence in the Jahangirpuri area, the use of predictive policing and facial-recognition tools raised concerns regarding the disproportionate targeting of Muslims, Dalits, and other vulnerable²² communities. Such practices may implicate Articles 14 and 15 of the Constitution of India.

According to Pound²³, Law is social engineering means a balance between the competing interests in society, in which applied science is used for resolving individual and social problems. As per his social engineering theory, the goal of the legal system is not only about safeguarding the people's rights but also to redefine social justice, order, and well-being. Especially ensuring the efficiency of existing law and well-defined foundries setup for to protect the interest of private, individuals, public.²⁴

From the perspective of natural law, the use of wide-ranging databases for AI decision-making may lead to bias, unreasonableness, discrimination, and unfairness, thereby

²⁰ J Vipra, ‘The Use of Facial Recognition Technology for Policing in Delhi: An Empirical Study of Potential Religion-Based Discrimination’ (Vidhi Centre for Legal Policy, 16 August 2021) <https://vidhilegalpolicy.in/research/the-use-of-facial-recognition-technology-for-policing-in-delhi/> accessed 17 Jan 2026.

²¹ Marda and S Narayan, ‘Data in New Delhi’s Predictive Policing System’ (FAT* ’20, 2020) 1–8 <https://doi.org/10.1145/3351095.3372865> accessed 17 Jan 2026.

²² ‘Special Teams for Probe, Delhi Cops to Use Facial Recognition’ *The Times of India* (16 April 2022) <https://timesofindia.indiatimes.com/city/delhi/spl-teams-for-probe-cops-to-use-facial-recognition/articleshow/90886017.cms> accessed 18 Jan 2026.

²³ Mani Tirupati BN, *Jurisprudence: Legal Theory* (16th edn, Allahabad Book Agency) pg.49.para 1.

²⁴ S Kumar, ‘What is Social Engineering?’ (iPleaders, 12 November 2015) <https://blog.iplayers.in/all-about-social-engineering> accessed 18 Jan 2026.

threatening rights such as privacy and the right to life. Through socio-economic approach express it affects especially vulnerable people's, Dalit's, Muslim's, dual nationality, immigrant, refugees, recidivist.

In the twenty-first century, the growing use of AI-driven tools can be justified only where a well-defined framework exists to address legal accountability gaps, socio-ethical concerns, and effective remedies. The AI-driven tools FRT, COMPAS, CMAPS, hiring algorithms lead to conflict with the international frameworks like UDHR²⁵, ICCPR²⁶. Leads to disproportionately targeted the Vulnerability reinforcing the racism, social biases society against the Art of 2 & 6 of UDHR and that Art 26 of ICCPR, in AI decision-making algorithm wide access of public data infringe the Art 12 of UDHR and Art 17 of ICCPR, Art 21 of Indian Constitution failure of the uphold the justice in *K.S. Puttaswamy v Union of India*²⁷ algorithmic bias, particularly in employment-related AI systems, may violate Article 23 of the UDHR, which protects the right to work and equal access to favourable conditions of employment, and is more appropriately examined under Articles 2(1) and 26 of the ICCPR, which embody non-discrimination and equality before the law and also the accountability gap leads to the inefficiency of effective remedy under Art 8 of UDHR, Art 2(3) of ICCPR and that of Art 32, Art 226 of Indian Constitution.

AI ethical principles play a pivotal role in establishing responsible, human-centric, and ethical use of AI. In global parlance, existing AI governance mechanisms such as New Zealand's Algorithm Charter and Israel's Artificial Intelligence Regulation and Ethics policy approach focus on risk-based assessment, transparency, and human oversight. Canada's Artificial Intelligence and Data Act remains part of an evolving legislative debate, while South Africa's National AI Policy Framework examines responsible AI through strategic pillars linked to developmental goals.

²⁵ United Nations, *Universal Declaration of Human Rights* (1948) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 17 Jan 2026.

²⁶ *International Covenant on Civil and Political Rights* (adopted 19 December 1966, entered into force 23 March 1976) 999 UNTS 171, Can TS 1976 No 47 [ICCPR].

²⁷ *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (India).

Principles safeguarding human dignity, fairness, explicability, and the prevention of harm are embedded in the EU Act, alongside with seven recruitment principles, including fairness, diversity, accountability, transparency, privacy, and socio-economic wellbeing, safety (*EU Ethics guidelines for trustworthy*). In contrast, OECD adopts through brief structure and five principles such as well-being, human-centric, accountability, robust-safety, explicability.²⁸

In the Indian context, AI governance relies on multiple general legal frameworks and sector-specific policy instruments rather than a single comprehensive AI statute. Digital harms such as deepfakes and unlawful content are addressed under the Information Technology Act, 2000, while identity fraud and consumer harms are regulated under the BNS, 2023 and the Consumer Protection Act, 2019. Recent policy developments, including India's AI Governance Guidelines and the RBI's Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) Committee Report, 2025, further demonstrate this sectoral approach, particularly in the financial sector. However, such fragmentation dilutes accountability and transparency in high-risk domains such as surveillance and predictive policing.

Further, India's emerging AI governance landscape is reflected in policy instruments such as the India AI Governance Guidelines, 2025 and sectoral initiatives such as the RBI FREE-AI Committee Report, 2025, which proposes a responsible and ethical AI framework for the financial sector. These developments show that India is moving towards risk-aware AI governance, but through a fragmented and sectoral model. Such fragmentation continues to dilute accountability and transparency in high-risk public domains such as surveillance, facial recognition, and predictive policing, where liberty and equality are directly implicated.

In *Manohar Lal Sharma v Union of India*²⁹, the Supreme Court underscored that privacy is not merely a statutory right, but also a constitutional and democratic right. The decision

²⁸ Organisation for Economic Co-operation and Development (OECD), *OECD Recommendation on Artificial Intelligence* (OECD/LEGAL/0449, 2019).

²⁹ *Manohar Lal Sharma v Union of India*, AIR 2021 SC 5396, (Pegasus spyware case).

emphasises the importance of privacy and data protection in matters involving surveillance. Broader, the case implicitly highlights through the appointment of the three expert special committee, the essence of enhancement cyber security measures, establish rights-based independent oversight and enact *sui generis* AI statute to balancing the security and privacy, the parliament enact or amend acts to ensure the democracy, transparency.

The Digital Personal Data Protection Act, 2023, read with the Digital Personal Data Protection Rules, 2025, represents a significant step towards governing digital privacy and operationalising India's personal data protection framework. The Act recognises consent-based processing under Section 6, the right to access information under Section 11, the right to correction and erasure under Section 12, the right of grievance redressal under Section 13, and the right to nominate under Section 14. It also deals specifically with children's personal data under Section 9. The 2025 Rules further operationalise parts of this framework by prescribing procedural mechanisms for notice, consent, exercise of data-principal rights, breach intimation, and the functioning of the Data Protection Board of India. However, the Act continues to face critical limitations. Section 3(c)(ii) excludes personal data made publicly available by the data principal or by any person legally obliged to make such data available.

Although the DPDP Rules, 2025 provide procedural detail for implementation, they do not create a dedicated regulatory framework for algorithmic surveillance, predictive policing, automated criminal-risk assessment, or autonomous decision-making. Therefore, the author's regulatory-gap argument remains relevant, but it should be positioned in light of the 2025 Rules rather than the Act alone.

Unethical access to, or use of, personal data by public authorities remains a concern because Section 17 of the Act permits exemptions in specified circumstances. The DPDP Rules, 2025 provide implementation mechanisms, including rules relating to children's data and the exercise of data-principal rights, but they do not substantially resolve the broader accountability concerns arising from State surveillance, AI-assisted policing, or automated decision-making.

Accordingly, the framework still requires additional safeguards for high-risk AI uses, including independent oversight, algorithmic audits, transparency obligations, and remedies for persons adversely affected by AI-based profiling. Although the Act and the DPDP Rules, 2025 strengthen India's personal data protection architecture, they do not expressly impose algorithmic explainability, bias-audit, or human-oversight obligations for AI systems used in surveillance and predictive policing. Sections 4 and 10 impose obligations upon data fiduciaries, but the framework does not specifically address how algorithmic systems should be assessed where personal data is used to generate criminal-risk profiles.

From the standpoint of fair and just administrative action, this gap is significant because algorithmic access to personal data may produce opaque, discriminatory, or disproportionate consequences. In contrast, Daniel J. Solove observes in the context of privacy and security that 'the distinction is essential to prevent government espionage from swamping the system we have in place to protect privacy rights and civil liberties.' He further cautions that espionage, though a necessary governmental function, must remain subject to oversight and public accountability. This observation highlights the importance of distinguishing between privacy and security in the context of public-data surveillance, particularly where such surveillance affects fairness and just administrative action.

VI. SUGGESTIONS AND RECOMMENDATIONS: SOLUTION-BASED JUSTICE MECHANISMS FOR AI-ASSISTED CRIME MAPPING

In the context of rapid technology change on AI reflects the essence of trustworthy AI with upholding societal communal, and UN Sustainable development and significance challenges. Through the implementation of responsible AI with the refined framework of AI Act lead Europe as a pioneer for the cut edge and ethical AI technology enshrine human-centric system.

AI becomes an integral part of daily life through visual assistance from health care to criminal attribution, education to employment - this influence on the principles of

Human rights concerns to the policymakers, developers and difficulties to anticipate harm, design effective remedy for the upcoming crisis.

Accordingly, through a victim-centric approach, this paper emphasises human dignity and proposes technical safeguards, public education, and foundational principles for framing an effective policy framework in the legal domain.

A. Technical Safeguards

This paper suggests that private-sector actors, including developers, software engineers, prompt engineers, programmers, and researchers, have a responsibility to build responsible AI systems. They must ensure that not to be harmful³⁰ or not contributing to human rights abuse.

Identify the outcome by means of input, to analyze direct and indirect harm, to ensure the participation of relevant experts to reconstructing the mechanism. If the system is used by the private and government sectors, both conducted the analysis for risk access.

During the creation and deployment of AI systems, developers must ensure accessibility, explainability, transparency, and clear information about how the system processes data. Third-party audits should also be mandated for high-risk AI applications in areas such as hiring, criminal justice, and lending. To establish an internal redressal mechanism with expert members for effective provision of remedy.

B. Curriculum Reform and Public Awareness

Widespread awareness-building and education are central to embedding human rights principles in AI systems throughout society. This requires AI education to go beyond introductory literacy by incorporating ethical values and encouraging community engagement with the effects of AI development on daily rights. Conducting government official programs must include practical case studies and hands-on experience in evaluating AI systems.

³⁰ UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (November 2021).

Mandatory instruction in AI ethics and human rights must be embedded within university and vocational curricula to prepare students to address bias, protect privacy, and design systems that uphold the dignity and autonomy of vulnerable populations.

At the same time, collaborative public awareness campaigns involving civil society, regulators, and public institutions should educate citizens about their rights in an AI-based society. Public-awareness campaigns conducted by public authorities and civil society must go beyond simple information dissemination and should enable citizens to understand, question, and seek remedies against harmful AI practices

C. Strategic Policy Guidelines

Recent Indian policy developments, including the India AI Governance Guidelines, 2025 and the RBI FREE-AI Committee Report, 2025, show that India is beginning to recognise the need for responsible, ethical, and risk-sensitive AI governance. However, the RBI framework is sector-specific and confined to the financial sector, while the MeitY guidelines operate as broader policy guidance rather than a comprehensive AI statute. Therefore, these developments should be treated as important but partial steps. For AI-assisted crime mapping and predictive policing, India still requires a dedicated rights-based framework that incorporates constitutional safeguards, human oversight, explainability, independent audits, proportionality review, and effective remedies for persons adversely affected by algorithmic decisions.

The proposed policy framework must be positioned in light of the DPDP Act, 2023 and the DPDP Rules, 2025. The Rules partially address procedural data-protection concerns by operationalising consent, data-principal rights, children's data safeguards, breach reporting, consent managers, and the Data Protection Board. However, for AI-assisted crime mapping, these Rules remain insufficient because they do not create a specialised framework for algorithmic accountability, predictive-policing transparency, automated-risk classification, or human-rights impact assessment. Therefore, India requires an additional rights-based AI governance framework, either through a dedicated AI statute or through sector-specific rules for high-risk AI systems used in policing, surveillance, criminal justice, welfare delivery, and public administration.

From the perspective of international legal standards, no AI system can effectively pursue a legitimate aim unless it operates within a well-established legislative framework. A legal framework incorporates with penalties, robust-safety delineated access control, authority mechanism, explicability, risk-based classification of AI leads to the effective law³¹. To frame such legal framework which explicitly defined how AI could be interact with human rights principles, reconceptualizing data privacy beyond conventional data protection through the technology-policy expert committee with domain of human rights experts, civil society actors, and representatives of vulnerable communities.³²

In legal parlance, autonomous AI surveillance may produce a “chilling effect” on democratic rights. Although the DPDP Rules, 2025 operationalise several procedural aspects of the DPDP Act, they do not sufficiently narrow the concern arising from Section 17 exemptions, particularly where state functions, investigation, research, archiving, or statistical purposes are involved. A robust framework must therefore ensure that exemptions are narrowly defined, proportionate, reviewable, and subject to independent oversight. In areas such as investigation, intelligence, supervisory functions, and predictive policing, unchecked immunity may result in false suspicion, wrongful accusation, misuse of personal data, and disproportionate targeting of vulnerable communities.

The framework must mandate expert human review before any adverse legal or policing action is taken solely on the basis of AI assessment. While the DPDP Rules, 2025 provide an important data-protection compliance layer, they should be supplemented by sector-specific AI rules requiring pre-deployment risk assessment, bias audits, explainability, audit trails, and periodic independent review for predictive policing systems. Strict statutory rules, mandatory training procedures for police officers, and rights-based operational protocols are necessary to ensure that AI tools remain assistive mechanisms

³¹ Organisation for Economic Co-operation and Development (OECD), *OECD Recommendation on Artificial Intelligence* (OECD/LEGAL/0449, 2019).

³² A Kumar Sood and S Krishna, *India AI Governance Guidelines* (Press Information Bureau, 5 November 2025) <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf> accessed 17 Jan 2026.

rather than substitutes for constitutionally accountable decision-making. To safeguard the rights of the people, there must be an additional level of administrative expert review board which consist various experts such as economic backward welfare, minority welfare, cyber security, technology expert to verify and rectify the action taken through the AI.

The legislative framework must enrich the constitutional principles by focusing on quality measurement rather than quantity measurement to ensure the public trust and transparency, surveillance measures must comply with the doctrine of proportionality and reasonableness, as held under the Supreme Court as *Modern Dental College v State of Madhya Pradesh*³³, any encroachment upon fundamental rights must satisfy four requirements such as sanction by law, legitimate legislative purpose, necessity, proportionality that extent must be essential not arbitrary to their restrictions.

In addition, the framework embodied with Human Rights centric Data Protection Impact Assessment (DPIA) such as Art 35 of GDPR³⁴ together with a jurisdictional grievance redressal mechanism to eradicate the unethical implementation and disproportionate harm caused to marginal people. No individual shall be subjected solely to adverse consequences based on AI assessment without prior human oversight.

To uphold the justice through the law, the framework must assign the joint monitoring bodies, mandatory transparency reporting, and independent audits to detect the discriminatory and unfair practices. These measures shall ensure that AI governance is aligned with universal norms of human dignity, International human rights instruments such as the UDHR, ICCPR.

VII. CONCLUSION

In crime mapping, the jurisprudential analysis on AI affirms that technological advancement is lacking in neutral value. Drawing from Kantian deontology and Pound's

³³ *Modern Dental College v State of Madhya Pradesh* (2016) Supreme court of India 7 SCC 353

³⁴ General Data Protection Regulation (GDPR) (gdpr-info.eu, 2026) <https://gdpr-info.eu/> accessed 17 Jan 2026.

theory of social engineering, AI governance must be anchored in duties, Ethical value, and the balancing of competing social interests. Ethics, though distinct from jurisprudence, infuses law with legitimacy by ensuring that AI systems remain instruments of human welfare rather than mechanisms of exclusion and control. The current fragmented regulatory approach in India exposes a significant accountability deficit, particularly in high-risk sectors such as surveillance and criminal justice, thereby undermining the effective remedies embodied in the maxim *ubi jus ibi remedium*.

In jurisprudential viewpoint upon the contemporary criminal administrative system, the AI-assisted crime mapping and predictive policing, as tools for efficiency and security. The AI has demonstrably amplified social inequalities when deployed without robust legal and ethical safeguards. Through the comparative analysis of COMPAS in the United States, SyRI in the Netherlands, and CMAPS in India reveal a reoccurring pattern as opaque algorithms biased due to historical data translate social prejudices into objective “criminal attributes,” resulting in disproportionate surveillance, arrest, and deprivation of rights of marginalized communities such as Dalits, Muslims, migrants, and minorities. For achieving International legal standpoint, the AI due process should resolve the conflict with constitutional guarantees of equality, dignity, privacy, and, as well as human rights norms under the UDHR and ICCPR.

In this legal cum technical context, predictive policing technologies have expanded more rapidly than the legal and democratic safeguards necessary to regulate them, creating a widening accountability gap. The strong and effective legal framework is required for preventing crime before its occurrence must not eclipse constitutional scrutiny, transparency, and judicial oversight. Without such legal safeguards, algorithmic predictions risk hardening into presumptions of suspicion against targeting marginalized communities.³⁵

Accordingly, the paper concludes that true and sustainable technological development lies not in unrestrained automation but in rebuilding public trust through human-centric,

³⁵ Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 Wash. U. L. Rev. 1109 (2017)

rights-based AI frameworks. This necessitates a constructive reform in domestic legal frameworks with risk-based classification and proportionate sanction, imposition of mandatory transparency, explain ability, and independent audits for high-risk AI systems; victim-centric grievance redressal mechanisms; and sustained public and professional capacity building on AI ethics and human rights.

For overcome all these legal complexities, if required, the new treaty should be drafted at international level or otherwise based on international legal standards, the new exclusive enactment come at national level. Only through such an integrated approach can AI-assisted crime mapping be reconciled with constitutional morality, international human rights obligations, and the foundational principle that justice must ultimately serve the interests of victimised persons.

VIII. BIBLIOGRAPHY

A. Cases

1. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
2. Manohar Lal Sharma v Union of India AIR 2021 SC 5396.
3. Modern Dental College v State of Madhya Pradesh (2016) 7 SCC 353.
4. State v Loomis 881 N.W.2d 749 (Wis 2016).

B. Legislation and International Instruments

1. Bharatiya Nyaya Sanhita 2023.
2. Constitution of India 1950.
3. Digital Personal Data Protection Act 2023.
4. Digital Personal Data Protection Rules 2025.
5. General Data Protection Regulation 2016.
6. International Covenant on Civil and Political Rights 1966.
7. Universal Declaration of Human Rights 1948.

C. Books

1. Berle I, Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images (Springer 2020).
2. Kant I, Groundwork of the Metaphysics of Morals (James W Ellington tr, 3rd edn, Hackett 1993).
3. Solove DJ, Nothing to Hide: The False Tradeoff Between Privacy and Security (Yale University Press 2011).
4. Tirupati Mani BN, Jurisprudence: Legal Theory (16th edn, Allahabad Book Agency).

D. Journal Articles and Academic Papers

1. Arts J and van den Berg M, 'What the Dutch Benefits Scandal and Policy's Focus on "Fraud" Can Teach Us About the Endurance of Empire' (2025) 45(1) Critical Social Policy 177.
2. Bolter JD, 'Artificial Intelligence' (1984) 113(3) Daedalus 1.
3. Chaturvedi, 'AI and Ethics: Jurisprudential Psychology to Investigate How Far It Can Be Regulated' (2025) 28 American Journal of Psychiatric Rehabilitation 784.
4. Ferguson AG, 'Policing Predictive Policing' (2017) 94 Washington University Law Review 1109.
5. Lee W, Hur J and Kim D, 'Examining Phishing Kits through Script-Level Analysis and Their Influence on Operational Phishing Websites' (2024) Proceedings of the ACM Asia Conference on Computer and Communications Security 1.
6. Marda V and Narayan S, 'Data in New Delhi's Predictive Policing System' (FAT* '20, 2020) 1.

E. Reports, Policy Documents and Institutional Materials

1. Centraal Bureau voor de Statistiek, 'Kenmerken van Gedupeerde Gezinnen Toeslagenaffaire' (2022).

2. Dienst Toeslagen, 'Toeslagen Herstel: Feiten en Cijfers' (2024).
3. National Center for Missing & Exploited Children, 'Generative AI CSAM is CSAM' (2024).
4. Organisation for Economic Co-operation and Development, OECD Recommendation on Artificial Intelligence OECD/LEGAL/0449 (2019).
5. Reserve Bank of India, FREE-AI Committee Report: Framework for Responsible and Ethical Enablement of Artificial Intelligence (August 2025).
6. Sood AK and Krishna S, India AI Governance Guidelines (Press Information Bureau, 5 November 2025).
7. UNESCO, Recommendation on the Ethics of Artificial Intelligence (November 2021).
8. Vipra J, 'The Use of Facial Recognition Technology for Policing in Delhi: An Empirical Study of Potential Religion-Based Discrimination' (Vidhi Centre for Legal Policy, 16 August 2021).

F. News Articles and Web Sources

1. Angwin J, Larson J, Kirchner L and Mattu S, 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks' ProPublica (23 May 2016).
2. Dastin J, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women' Reuters (10 October 2018).
3. Drolia R, 'Chhattisgarh: IIIT Raipur Student Held for Morphing Photos of Fellow Girls Using AI Tools' Times of India (9 October 2025).
4. Kumar S, 'What is Social Engineering?' iPleaders (12 November 2015).
5. 'Special Teams for Probe, Delhi Cops to Use Facial Recognition' The Times of India (16 April 2022).