INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE CULMINATION OF ARTIFICIAL INTELLIGENCE AND DATA PRIVACY: A SCRUTINY FOCUSED ON HUMAN RIGHTS HIGHLIGHTING PROFUNDITY OF DIGITAL WRONGDOINGS AND MACHINERY SUPERVISION

AUTHORED BY - ANANYA SAHA

Profession- Advocate at High Court and District Court of Agartala, Tripura

Abstract

In this paper we shall discuss about how with the emergence of Artificial Intelligence especially those of prolific nature, there has been an increment in trepidation among all and how digital technological developments like Social Media Algorithms, Search Engine Operation, Analytical Database tools, Augmented Reality (AR) and Virtual Reality (VR) and many other digital productions have resulted into both positive and negative outcomes, like AI potentially addresses complex issues related to the advancement of education, improvising health facilities, climatic perceptions and scientific innovative action but there is a major concern regarding data privacy because it was developed with the view of safeguarding personal details of individuals and different associations by empowering them to have a supervisory control on their own data. Along with that the paper also focuses on the impact of one of the finest regulators in today's modern society, which is ChatGPT whose training database increased its area of parameter from 1.5 billion to 175 billion within a year. However, in the growing digital world major concern has been raised regarding empowerment of Artificial Intelligence and data privacy. This ultimately represents significant conveyance of performance capability by machines similar to that of human intelligence. The paper also highlights about the rights provided by the Constitution of India to its people to safeguard their privacy and safety blending with the recent development of ChatGPT and Open AI. Undoubtedly such advance technologies have been a boom to nation and its people but this fact cannot be denied that it has been an entry pass to various online crimes. Therefore, this usually lacks efficient method of operation with no meaningful signs of guarding or monitoring its aftermath. The conclusion summarises the key ideas covered, emphasizes how important AI is to advance data security and privacy, and call for more research, study and development.

KEYWORDS: *Artificial Intelligence, Data privacy, Digital Wrongdoings, the Constitution of*

ISSN: 2582-6433

India, Social Media Algorithms, Human Rights

CHAPTER-1: INTRODUCTION

1.1. The epoch of artificial intelligence

The term "Artificial Intelligence" was first coined by Mr. John McCrthy. It is a domain of computerised database which aims at producing technological developments for performing distinct tasks that are generally executed by manpower. These programs are almost replacing human capability of performance through their intelligence, audio-video adaptability, learning and adapting, developed system of reasoning, pattern observation and supervisory techniques. AI is potentially expedient in transforming every kind of commercial enterprise to benefit the society at large. This basically functions through data collection which poses some risk to security concerning privacy. The information are usually gathered from numerous intentional sources, like when personal data are being furnished by people themselves or unintentional sources where information are collected without individuals even realising the matter, such data might end up being utilized in a very unexpected way.

The development of different technological creation were of great advantage but in the early 20th century Aldous Huxley warned everyone through his book 'Brave New World' whereby he stated that we, the homo sapiens might enter into a different unusual world of monster or superhuman with the advent of genetic innovation. The origin of AI and other mechanisms related to it accelerated the drive for cyber security, showcasing two sides of a coin 'technological advancement and cybercrime', rising concern for coming up with strategies to avoid it from falling into wrong hands because there is an augmented collection and utilization of personal data questioning authenticity and reliability of privacy in the modern digital pool.

One of the most usual challenges faced by the users of AI technologies is 'right to privacy'. This particular right has been considered to be a fundamental right in the case of K.S Puttaswamy vs. Union of India (2017)[1], but present legal provisions of India do not fully regulate the impact of AI on the privacy of individuals. This is because certain questions like who regulates AI-generated data? Who shall be liable for data infringement in the operation of AI technologies? What are the procedures adopted for transparent decision making of AI systems? , all these issues remain unresolved. Therefore, there is a need of balanced norms for AI governance, ensuring alignment between India's innovative AI algorithms, privacy rights and ethical and accountable mechanisms.

[1] AIR 2017 SC 4161

ISSN: 2582-6433

1.2. Research Problem

The present research study has been conducted with the view to address the following problems:

a. Problem associated to dissolving of public's sensitive data in the pool of cyber risk.
b. Problem associated to lack of proper encrypted security and unauthorised access to personal data.
c. Problem associated to the breach of the rights granted by various international and national instruments.
d. Problem associated to vulnerability of AI showing such mechanisms themselves prone to cyber attacks questioning authenticity and reliability of such system.
e. Problems associated to the maintenance of the legal frameworks related to data privacy and other protections provided under the Indian Constitution

1.3. Research Objective

This paper has been written to meet the following objectives:-

- To understand the meaning of the mechanism of AI and the problems associated with it.
- To know the regulations drafted globally to protect the rights of the humans and evaluate them with the emergence of AI in the realm of digitalism.
- To analyze the techniques developed to preserve data privacy and avoid risks.
- To comprehend the disadvantages brought by the emergence of AI.
- To understand the strategies brought by the policymakers to monitor sensitive information.
- To understand the legal frameworks provided by the Indian Constitution for privacy maintenance.

1.4. Research Questions

i. Whether the data of the public at large displayed on different online platforms for multiple purposes are secure enough from falling into the trap of cyber risk?
ii. Whether proper security has been encrypted to protect the personal data from any kind of unauthorised access?
iii. Whether Artificial Intelligence is violating privacy concerned laws developed by various international and national instruments to protect rights of the individuals?

ISSN: 2582-6433

iv. Whether the mechanisms associated with artificial intelligence are strong enough to protect itself from the risk of cyber attacks?

1.5. Research Hypothesis

The purpose of this study is to analyse the concept of **"Artificial Intelligence and Data Privacy"** and its relevance in the society. The study tries to answer the question as to huge data collection posing potential risk to security concerning privacy. The researcher encompasses the paper with techniques to preserve data privacy so that people are not denied their freedoms like freedom to expression, religion etc. Further, an analysis has been made on digital wrongdoings highlighting the fact that how convenient it has become to commit a crime by using AI technologies with less fear and more possibility. AI is being utilised to disseminate false information by using sentiment analytical tool to artificially influence market sentiment by searching news websites and social media. A number of rights have been harmed due to the culmination of distress to privacy caused by the advancement of AI. Therefore, cybercrime, data privacy and AI are parts of the same cycle and one has to look into all the three so that none is violated during implementation.

1.6. Research Methodology

The methodology opted for carrying out the recent work is purely doctrinal in form. The researcher has relied upon various primary and secondary doctrinal sources. The researcher has analysed every facts of this paper by referring various websites, statutes, books, articles, and research papers. The paper has been discussed with existing legal provisions and all the relevant information have been framed within different chapters for better and clear understanding of the readers. The doctrinal study of the different conventions, statutes and other legal updates proved to be sufficient enough to achieve the objectives of the research. To preserve the scholarly legitimacy of the deliberation, an enormous priority has been placed on citing and due credit has been provided to all the papers that are referred to while conducting the present research analytical study.

The overarching intent of doctorial juridical study is to comprehend the fundamental tenet that inform legal decision-making by examining current principles of justice, provisions of law, and court decisions. For acquiring profundity of laws in a particular field, it requires thorough reading of academic publications, court ruling and various other documents associated to law. Legal researchers as well as the professionals employ the data obtained by this research to determine trends, evaluate the coherence of legal concepts within a particular territorial region

ISSN: 2582-6433

and comply with and implement legal regulations. It is an essential apparatus for constructing legal arguments and determining making of different policies and legal procedures.

1.7. Literature Review

I. ARTIFICIAL INTELLIGENCE AND PRIVCY

a) A threat to privacy: *Sunitha Abhay Jain and Simran Jain*

The work on the particular paper is focusing on the genre that there exists serious concern about the possible risks to personal data when artificial intelligence and privacy emerge on the same note. Further, it suggests that the vast amounts of data collected and analysed should be handled properly through proper adherence to the national and international frameworks established for the protection of human rights. Further a discussion has been made on the relevance of Article 21 of the Indian Constitution on maintaining privacy. Thereafter, an emphasis has been placed upon the fact that India lacks proper legislation regarding data protection and efforts are greatly needed to come up with specific laws focusing on the same.

(Jain, S.A., Jain, S.A., 2018. Artificial intelligence: a threat to privacy. Nirma ULJ, 8, p 21.)

b) Privacy risks associated with AI

- **Data gathering and processing:** The paper brings out the observation that AI frequently needs enormous volumes of personal details, gathered without user permission which results in being used without authorization (Sandhu et al., 2025).
- **Determinations from data:** The paper focuses on the event that AI has the authenticity to deduce private information from allegedly innocuous data, such s gender or race, raising the possibility of privacy infringement (Jurewicz et al., 2024)
- **Unfettered implementation:** The paper focuses on the demonstration made by social media and tracking tools regarding the quick and uncontrolled adoption of AI technologies across range of industries might increase privacy problems. (Jurewicz et al., 2024)

c) Mitigation strategies

- **Data security tools:** The fact that certain dangers related to particular elements of AI can be decreased by putting tailored privacy protection technology into practice has been highlighted in this paper.(Curzon et al., 2021)

ISSN: 2582-6433

- **Regulatory frameworks**: In this paper a great emphasis has been given to the analysis that in the era of artificial intelligence, safeguarding privacy rights requires the establishment of strong regulatory frameworks and moral standards.(Joshi, 2024)
- **Cooperative Efforts:** This research has been made to ensure sustainable research and application of AI systems, entities must cooperate to strike a balance between the advantages of AI and the requirement to protect the rights relating to privacy. (Joshi 2024)

  AI proposes prospects for progress in safeguarding privacy systems even if it poses serious issues with confidentiality. For an absolute certainty that the advantages of AI are not conferred at the expense of people's right to privacy, more study and additional research in this arena of study is essential. (Jain & Ghanavati, 2020)

II. FREEDOM OF EXPRESSION AND PRIVACY

a) Privacy and Freedom of Expression in the Age of Artificial Intelligence

The paper highlights the fact that the act of freedom of expression requires privacy, because without it, people will be unable to express themselves forbidding them from enjoying their right to free speech. Further, the paper holds a detailed analysis on the nexus formed between AI, privacy and freedom of speech and expression. Also, it keeps certain key notes on article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) along with the related issues brought by the advancement of AI. Therefore, various industry initiatives have also been discussed as a response to the ethical and legal questions posed by AI like 'Global initiative on Ethics of autonomous and Intelligent Systems of the Institute of Electrical and Electronics Engineers (IEEE)' etc.

Privacy International and ARTICLE 19, 2018. Privacy and freedom of expression in the age of artificial intelligence

b) Effect on Freedom of Expression

- **The growth of empowerment with AI:** The paper shows that AI can assist freedom of expression by facilitating the exchange of various viewpoints and enhancing information access (Giovnni & Pietro, 2023).
- **Information management threats:** This paper brings forth that AI mechanisms frequently review information according to preset rules, which might result in the elimination of acceptable expressions and produce "filter bubbles" that restrict accessibility to different perspectives (Kolrevic, 2022).

ISSN: 2582-6433

c) **Privacy Concerns**

- **Regulating frameworks:** An effective suggestion has been made in this paper stating strong privacy regulations are necessary to uphold people's rights and promote technological advancement. It's critical to strike a balance between the evolution of AI and protection of personal details (Pawlak, n.d.).

III. LEVERAGE OF DEEPFAKES BY AI FOR IDENTITY FRAUD

The paper works on the concept that fake videos are getting converted into realistic videos using machine associated with AI (Dhiman, 2023).The growing threat of deepfake films has led to the development of numerous techniques for identifying them during the past ten years. However, the main problem with these processes is that they are laborious and incorrect. An analysis has been conducted that raises concerns about digital identity theft, which is illegal in the majority of nations, including India, where it has been addressed in the digital environment under the Information Technology Act. (Subramanian V & Swathi, 2024)

IV. EVOLUTION, RISKS, AND RESPONSES TO AI-POWERED CRIMINAL ENTERPRISES

The work shows a detailed analysis on the field that with a sharp surge in events, including a 238% increase in computer-generated attacks in 2023, artificially intelligence-powered digital assaults have demonstrated a 67% higher accuracy rate (Reddem, 2024). Further, focus has also been invested on the legal frameworks developed to address the ethical ramifications of AI in criminal activity, investigating the allocation of blame when AI becomes involved (Panattoni, 2025)

CHAPTER -2: GLOBALLY RECOGNISED HUMAN RIGHTS AFFECTED BY ARTIFICIAL INTELLIGENCE IN THE REALM OF DIGITALISM

Human rights are comprehensive and sacrosanct rights that are conferred upon every individual notwithstanding to their gender, nationality, religion, caste, race or any other position in the society.

Below mentioned are the human rights that are impacted by the emergence of AI in the realm of digitalism. These rights are largely incorporated in three major documents forming the

ISSN: 2582-6433

foundation of international human rights law known as the 'International Bill of Human Rights'. These documents include the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR).

I. Right to life

Article 6 of ICCPR grants the following:

- Everyone is entitled to right to life.
- Death penalty may be imposed only for serious crime as per law in force at the time of the commission of the offence.

II. Right to liberty and security

Article 9 of the ICCPR states the following:

- It grants right to liberty and security to every individual.
- Forbids arbitrary arrest and detention of anyone.
- Forbids deprivation of liberty except on grounds and procedure established by law.

III. Equality before the Courts

Article 14 of the ICCPR states the following:

- Everyone shall be equal before the eyes of the courts and tribunals.
- While determining criminal charge or of his rights and liabilities in a suit, the person is entitled to fair trial by a competent, unprejudiced and independent tribunal established by law.

Threats: The expanding utilisation of AI in the administration of criminal justice has made the right to personal liberty more prone to exploitation. One such case includes the use of 'recidivism' a risk-analysis software used in the U.S penal proceedings for procedures involving information of detainment ordinances to the concerned persons, providing bail in criminal conviction etc[2]. Due to this software, black suspects have been wrongfully classified as high risk, imposed harsher bail requirements, detained pending trial, and given lengthier prison sentences. This software is marketed as a device for impeding evaluation of criminal risk by assisting the judges in their penalty

[2] Angwin et al, *Machine Bias*

ISSN: 2582-6433

decisions. However, ascribing a degree of future guilt to an accused based on their probability of re-offending- whether high or low- could compromise the assumption of innocence inevitable for a fair trial.[3]

Prediction regulating software usually threatens imposing of wrongful guilt, by creating a bias view in the minds of the executing officers using the past records. Although numerous courts depend largely on the result since the software is perceived as impartial, reports indicate that judges lack adequate knowledge as to how risk analysis algorithm operate. Because of this, it becomes unclear if court rulings based on this software may actually be regarded as fair.[4]

IV. Rights to privacy and data protection

Article 17 of ICCPR, Article 7 and Article 8 of the EU Charter of Fundamental Rights contain regulations protecting personal data of a person, ensuring respect for his private life and preventing unlawful interference with his privacy and dignity.

Right to privacy is a fundamental right for human existence. The right encompasses other rights like right to freedom of expression and to form association.

Threats: AI operations are often conducted to assess the large data collected through its algorithms, in order to create feedback database and enhance its mechanisms. But this gathering of big data hampers people's privacy and puts data confidentiality at risk. Such process of data inspection may divulge personal data of a person, which were required to be protected being sensitive in nature even if acquired publicly. For example, ML Models have been developed in order to provide information related to a person's age, occupation, gender and marital status with an exclusive utilisation of cell phone location.[5]

V. Right to freedom of thought and expression, religion, assembly and association

Article 18 of ICCPR and Article 18 of UDHR grants every individual the freedom to adopt any religion of their choice irrespective of private or public platform without any kind of coercion which could impose a barrier on such freedom.

[3] The Committee of Experts on Internet Intermediaries; Algorithms *and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, COUNCIL OF EUROPE, 10-12, March (2018), https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

[4] Robert Brauneis and Ellen P. Goodman, *Algorithm transparency for the smart city*, 20 THE YALE JOURNAL OF LAW AND TECHNOLOGY, 103-176 (2018)

[5] Steven M Bellovin, et. Al, *When enough is enough: Location tracking mosaic theory, and machine learning,* NYC JOURNAL OF LAW AND LIBERTY, 555-628 (2014)

ISSN: 2582-6433

Article 19 of the ICCPR talks about individual's right to express their view and hold their own opinions without any interference. Such expression of views or holding of opinion includes seeking, receiving and imparting of information in any form, orally, in written, in print, or in the form of art or any other forms of media as per his convenience.

Article 20 and 21 recognises the right of peaceful assembly along with the freedom to form association with others. The only restrictions which could be imposed include those prescribed by law and are necessary to maintain national security, public order, public health etc.

Threats: The system of AI is used by the digital organisations to flag certain posts that are claimed to violate their terms of service. Governments usually exert pressure on these companies to fix issues alleging contents spreading hatred, promoting terrorism, and circulating fake news, but such pressure from the concerned authorities lack proper standards or strategies, which has ultimately increased the use of automated mechanisms.[6]

For example, In Germany a recent provision has been passed requiring social media sites to remove every kind of flagged contents within a period of 24 hours or seven days for those lacking clarity.[7] But similar to any other digital mechanism artificial intelligence also lacks perfection and due to the exerted pressure of quick removal of certain questionable contents, much of them are taken off in error.

Since right to privacy is questionable in today's world of artificial intelligence, people's freedom to express their views or opinions (subjected to restrictions) is also being affected. People are now being cautious due to the discomfort thinking of being watched or absence of anonymity creating an atmosphere of serious repercussions on freedom of expression.[8]

VI. Right to Education

Article 13 of ICESCR provides that all the members to the present convention

[6] FREEDOM HOUSE SURVEY FOUND 30 OF 65 OF GOVERNMENTS ATTEMPTED TO CONTROL ONLINE DISCUSSIONS. https://freedomhouse.org/article/new-report-freedom-net-2017-manipulting-social-media-undermine-democracy (last visited Oct 28, 2025)

[7] *Germany starts enforcing the speech law*, THE BBC, January 1,2018, (last visited Oct. 6, 2025) https://www.bbc.com/news/technology-42510868

[8] Privacy International and Article 19, *Privacy and Freedom of Expression in the Agen of Artificial Intelligence,* April 2018 (September 30, 2025, 4:30 PM) https://privacy international.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age %20of%20Artificial%20Intelligence.pdf.

ISSN: 2582-6433

recognizes right to education by stating that primary education is compulsory and freely available to all, everyone should have widespread accessibility to all forms of secondary mode of education, including professional and career-oriented education, through all suitable channels, including the gradual implementation of free education. It also provides that for individuals, who were unable to finish their primary education, they must be provided basic education facilities as far as feasible.

Threats: AI has the potential to impose serious transgress on the principle of equitable access. American universities are utilising stochastic computational systems to suggest candidates for admission. These are frequently made to comply with the school's inclinations, and have numerous problems that can cause prejudice, such as the implication of historical information from students who have already been admitted, to help guide the model. Given that, numerous prestigious universities have traditionally been frequented by affluent white men, and any model that utilises these facts run the risk of reproducing historical patterns. In decades to come, these systems would probably use machine learning which would make it more difficult to detect partiality. This might led to discrimination by colleges masquerading as impartiality.[9]

CHAPTER-3: PRINCIPLES FOR GOVERNING ARTIFICIAL INTELLIGENCE

Proper governance requires certain fundamental principles, so do artificial intelligence. Therefore, mentioned below are the vital principles which need to be adhered to while operating AI:

a. **Free consent:** Individuals must be given proper opportunity to provide their free consent for valid collection and utilisation of data by various organizations in the mechanism of AI. Any kind of coercion must be avoided so that transparency and legibility could be maintained also users should be given the right to withdraw their consent at any point of time.

b. **Transparency:** Organisations are required to maintain a transparent interaction with its users by providing clear and simple knowledge for the purpose, extent and impact of the collection of data, so that a relationship of trust could be ensured and people would become more aware regarding the utilisation of their data.

[9] O'Neil, Weapons of Math Destruction, 50-67

ISSN: 2582-6433

c. **Fairness:** Organisations must assure fair and unbiased use of methods in AI systems by addressing issues like algorithm bias and unequal outcomes through proper evaluation of the maintenance of fairness in the entire lifecycle of AI models.

d. **Accountability:** Organisations collecting data to use it for generating AI outcomes should be accountable enough to take certain responsibilities like maintaining data accuracy, integrity, adopting security measures, and resolving issues like algorithm bias and prejudice impacts.

e. **Security:** Organisations should aim at implementing strong security measures to prevent the data from getting used for malicious activities. Such measures include encryption, regular safety audits and restrictions on access. So that data infringement and unlawful access could be avoided.

f. **User supervision on their data:** Organisations should aim at providing individuals with controlling power over their data which are applied into AI system. This includes the power to access their data, to adapt modification and power to delete their data whenever required, along with the ability to quit their availability of data from the AI system.

CHAPTER-4: AN ANALYTICAL NEXUS BETWEEN AI AND PRIVACY RIGHT IN THE ERA OF INTERNET

The liberty to enjoy privacy rights is considerably pertained to the application of AI technologies. Since technology is upgrading at a rapid pace artificial intelligence is being utilized more progressively in numerous aspects of our lives and this advancement of AI has the potential to completely transform the way of using technology.[10]

The right to privacy is the protection of one's personal data from prying eyes. Confidentiality is essential because it keeps people safe from identity fraud, preserves their autonomy, respect, integrity, gives managing power on their personal details, enjoys free consent and keeps free from concern of being under scrutiny.

In the digital age, private information has grown in value. The quantity of data we produce and disseminate online is increasing at a steady pace, allowing distinct organizations to execute these data to come up with better decisions and obtain new perspectives. A person's private realm now encompasses more than just their concrete private existence due to the growing

[10] Nick Lawrence, *AI in UI, 2323 and Beyond*, MEDIUM (28th August, 2024)(last visited Oct 29, 2025), https://uxplanet.org/ai.in.ui-2023-and-beyond-346b4602eff7

ISSN: 2582-6433

prevalence of digital mechanisms in day to day life and the impact of both the real and virtual environments respectively.

AI systems are getting used in numerous strategies that disrupt the privacy domain in addition to rely heavily on the individual's confidential details for their advancement. As a result, privacy has grown to be a critical concern in the modern era. AI is becoming a necessary tool to assist people regulate their hectic schedules and do their respective professions more quickly and effectively. Large volumes of information are vital for AI to train its algorithms and enhance efficiency, problem-solving techniques and forecasting. The possibility of data infringement and illegal acquisition of personal data are the primary security concerns associated with AI.

There prevail certain risks that the information gathered, analyzed and preserved could end up landing in wrong grips due to illicit activities like hacking or other security lapses. Consequently, there is an apparent violation of the right to privacy.[11]

CHAPTER-5: PRIVACY CONCERNS IMPOSED BY AI

The development of AI has posed various challenges. Some of them have been discussed below:

a. **Unlawful utilisation of personal data:**

AI gathers information from multiple cradles; many of them gather those data without the knowledge or consent of the concerned users.

The technology of AI might scratch data from the photos which are posted online, various soil media handlings, fitness tracker gadgets, CCTV footages, purchase histories from various applications and every digital interaction that can be used to operate AI applications through input of massive data.

The value of AI relies on its capacity to identify designs indistinct to the human eyes, through these acquired data; predictions are made about users which are ultimately produced as outcomes. Therefore, AI holds the ability to generate information that is otherwise challenging to be accumulated easily or is still not in existence; showcasing that information collected may be used beyond the extent for which there was grant of actual permission given by the concerned person.

[11] Dr. Mark Van Rigmenam, *Privacy in the age of AI risk, challenges and solution,* www.digitlspeker.com (22 August 2024) (last visited Oct 29, 2025)

ISSN: 2582-6433

b. Prejudice and discrimination in the algorithms of AI

AI's potential to make biased decisions that disproportionately impact particular groups is yet another privacy concern to look into. If the data utilized for instructing the AI is discriminatory, it may bias against specific groups when it comes to employment or any other factors.[12] Prejudice datasets used for developing AI's algorithms have the potential to perpetuate current disparities and produce discriminating results in the workplace, medical care facilities and legislative bodies. For instance, considerable worries have been found regarding AI-generated financial security procedures in South Africa because this unfairly discriminates against those with lesser incomes. Similar concerns have surfaced in Asia, especially in relation to execution of AI mechanism in China for community credit assessments, which might unjustly impose sanctions on vulnerable section of the society.

Therefore, digital prejudice is growing to be a significant issue, as a large number of decisions are made by mechanisms that rely on artificial intelligence methods like machine learning, chatbots etc. Further, biased computational judgments perpetuate societal injustice that is already experienced by underprivileged groups and such human discriminations results in unfair and possibly dangerous consequences from AI systems.[13] Hence, it takes significant thought to resolve bias in AI at every stage of the process.

c. Unawareness of the techniques adopted while converting data for using it in AI

Several individuals engage with AI computational programming on a daily basis through engineered suggestions, social media sites, and various web searches, but many of them are ignorant of the procedure adopted by such mechanisms to prioritize and analyze data. According to various research findings, only users with advanced technology comprehend this on an entire basis. There is an inadequacy of knowledge on the fundamental techniques, algorithms, and methodology that assist in making artificial intelligence conceivable. Embracing and administering AI appliances can be difficult due to disparity caused by lack of understanding, which affects both the individuals' and enterprises.

Also it is to be noted that knowledge must constantly be updated due to the quick development of AI system, particularly with developments in generative form of AI.

[12] Yancy Dennis, *Artificial Intelligence- privacy and ethics,* MEDIUM (28th August 2024) (last visited Oct 29, 2025), www.medum.com

[13] Alexandra Jonker & Julie Rogers. *What is algorithmic bias?* IBM (Oct. 28, 2025, 3:47 PM), https://www.ibm.com/think/topics/algorithmic-bias

ISSN: 2582-6433

d. Lack of transparency between individuals and AI mechanisms

Algorithmic AI relies on the quality of the data used for training the model, much like any other data-powered mechanism. Considering the possibility of algorithms getting susceptible to prejudice in the data, their utilisation carries certain inevitable hazards. Gaining the trust of consumers, authorities, and others impacted by computational decision-making requires transparency to a great extent.

On a frequent basis AI programmers prefer not to adhere to transparency frameworks. The very primary cause for such non-adherence is maintenance of their dominance edge. Particularly when it comes to IPR, AI developers are not in the favour to share their programming computations and decision-making procedures with their rivals because they consider them as a unique characteristic that secures them an advantage to exercise power over them. Due to this reason information are frequently kept secret from both the public and the appropriate supervising agencies. Another reason for not maintaining transparency is the fear of not adhering to the intricate and complicated legal framework in some regions of the world, particularly in the EU.[14] Therefore, for all the reasons mentioned above information are not made transparent to the public at large highlighting the fact that there is a lack of conveying a thorough grasp of the characteristics and constraints of the system to the stakeholders embracing that the concept of transparency is the possible means of enhancing the trust of individuals on AI systems.

CHAPTER-6: INSTALLATION OF CERTAIN TECHNIQUES TO MINIMIZE PRIVACY RISKS.

1. Limitation in collection of data:

Personal data should be collected with the consent of the concerned person within a limit of necessity through lawful, fair and justified means.

The vital characteristics of various AI systems exclusively machine learning operates by conducting training and tests on the huge amount of collected data. Though massive collection of data assists in the development and operation of AI mechanism but such measure can directly contradict the policy of limited collection.

Digital advancements in multiple mediums like IOT devices, smart phones, laptops,

[14] Vera Lucia Raposo, *How is 'Unexplainable' and Non-transparent AI affecting Healthcare Delivery?*, 11 SPECIAL ISSUE: AI AND ROBOTICS IN HEALTHCARE SCIENTIFIC PUBLICATION, 1, 2-8 (2024)

ISSN: 2582-6433

and web tracking gadgets shows that all information inserted into AI technologies are not gathered through traditional form whereby data used to be collected with the consent of the person. In fact, at times individuals aren't fully aware of whatever personal data is being collected from their devices and inputted into AI systems. Therefore, the principle of limited collection tries to impose a barrier in data collection in order to lessen privacy concerns.

2. Specification of the purpose behind such collection

   A proper explanation behind the purpose of collecting personal data must be given in the form of collection notice to the concerned persons. One of the most substantial challenge to this principle is AI using data beyond the purpose for which it was collected initially i.e., an excessive collection of personal information beyond necessity making huge number of collection notices and ultimately questioning policies related to privacy in an attempt to gather every data. So that digital mechanism of AI could be utilised to specify individual's preferences regarding how and to what extent their personal data should be utilised.

   Therefore, user's privacy preferences should be focused on and different conditions must be implemented while collecting data. In this manner AI could play a significant role in the development of individualised preferred model whose potential would completely implement transparency, consensual supply of information and a proper adherence and maintenance of privacy provisions.

3. Restriction and minimisation of data utilisation

   In digitalism, the purpose behind the collection of personal data is classified into two groups- primary and secondary purpose.

   Primary purpose is the one for which the data is mainly collected and secondary purpose is the one which is 'reasonably expected' by the individual to be used for. This gives rise to dispute concerning whether the data inputted into the system can be held to be 'reasonably expected secondary purpose' because in various cases result of inserting such data would be known to the individual. The system of AI can culminate distinct patterns and data associations which re unpredicted by humans, revealing such information to new potential users.

   Therefore, organisations making use of such information find it difficult to provide assurance while using AI technologies that such personal information will only be used for the purpose for which it was collected. This means, due to the technology growing ubiquitous and people's reluctant behaviour towards privacy especially those belonging

ISSN: 2582-6433

to the age of 18-24, use of personal data for only reasonably expected secondary purpose is no more maintained.

Hence, certain barriers must be set in the utilisation of personal data by AI through proper mechanism.

4. Development of strong methods for governing individual data

   Strong governing methods ensure that the privacy laws are maintained properly and personal information are protected from unlawful and unfair practices long with preventing them from misuse.

   Such methods include certain key components such as categorisation of data access control mechanisms, and regular audits in order to meet proper standardization. The concerned organisations are required to make their practices comply with the industry guidelines such as GDPR or CCPA that sets the proper criteria for data interpretation. For implementing such practices multiple processes get involved like defining roles and duties to be adhered to in such governance, training of employees etc., and finally, comes the leadership whereby accountability and proper enforcement of the concerned methods are looked upon actively so that sensitive information are protected building relationship of trust and transparency with the public at large.

5. Use of Virtual Private Network

   For an effective protection of personal data customers must consider using VPN networking site for encrypted internet connection, so that third parties find it difficult to track online activities of individuals. Also, individuals are required to have awareness regarding latest privacy and data protection laws so that they can fully safeguard their rights.

   Therefore, staying updated regarding potential risks and knowledge of tools available to protect rights of individuals will give manpower to exercise supervision on their digital foot prints and ultimately minimizing exposure to data infringement would create a better digital environment.

CHAPTER-7: PRIVACY LAWS RECOGNISED IN INDIA IN LIGHT OF ARTIFICIAL INTELLIGENCE

AI is transforming a number of sectors including government, banking and medical care. However there are serious considerations about data protection due to its quick evolution.

India's main legislative framework managing data privacy is 'The Digital Personal Data

ISSN: 2582-6433

Protection Act, 2023 (DPDP Act)', which attempts to control the administration of confidential data by organizations utilizing AI. Certain principles including objective restriction, user permission and data optimization are introduced by the DPDP Act. The Act is extremely pertinent to AI technology that deal with massive amounts of personal details since it addresses the procedure through which data can be gathered, preserved, analyzed and disseminated. Nevertheless, the Act lacks particular combat towards issues related to AI, like algorithm biasness, recognition of profiles, automated decision-making. This implores a query to determine whether current legislation is adequate to control data analysis driven by AI.

Furthermore, regulations like Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, though not specifically mentioned but to certain extent provide protections to data.

Additionally, sector-specific regulators like Reserve Bank of India (RBI) and Securities and Exchange Board of India (SEBI), as well as regulatory organizations like Data Protection Board of India (DPB), are essential in guaranteeing conformance.

CHAPTER-8: DIGITAL WRONGDOINGS THROUGH AI

The potential risks associated with AI technology are growing along with its sophistication and capabilities. In this paper, a summary of crimes has been mentioned that were facilitated or made feasible by AI in the following years, also the potential severity attached to these risks have been discussed. Particularly noteworthy in relation to illegal activities re generative AI's capabilities to help with programming generate output that appears authentic and produce vast amounts of data in a rapid pace. Unfair and prejudice, breaches of confidentiality, security threats, fictitious data and imitations are certain significant domains to be looked into.

AI advancements increase the effectiveness of many conventional criminal activities. For instance, trading markets can be carried out with greater effectiveness by utilising AI's machine learning tools, in order to examine and take advantage of monetary data and spear phishing grows its credibility with autonomous tailored emails.[15] Therefore, with the aid of AI, malware computer programming assistants have been created, through which crimes that were previously unattainable have now become feasible by several wrong doers.

Another important future aspect has also been discussed in this paper, which includes the

[15] *The Rise of AI-Enabled Crime: Exploring the Evolution, Risks, and Responses to AI-powered Criminal Enterprises*, TRM BLOGS (Jan 29, 2025) (last visited Oct 28, 2025) https://www.trmlabs.com/resources/blog/the-rise-of-ai-enabled-crime-exploring-the-evolution-risks-and-responses-to-ai-powered-criminal-enterprises

ISSN: 2582-6433

evolving of 'fresh types of illegal activities' that either directly or indirectly take advantage of AI technologies. Cyber attacks against AI mechanisms to tamper with their resultants for recipients and malicious attacks on automated vehicles, where AI methods are employed to operate applications to cause distress, are two illustrations. AI has the potential to completely change certain offenses making them new hazards that society will have to deal with. For instance, sophisticated malware driven by AI can amend and adapt to avoid being identified, posing a threat to the protection systems in place.

1. Evolution of malware and cyber hacking:

   It is often warned by security personnel that AI-based applications have the potential to drastically reduce the entrance impediment for digital criminal activities, enabling less proficient customers to execute complex operations.[16]

   Offenders can consult specialized LLMs for assistance in generating efficient malware rather than requiring sophisticated programming knowledge. For instance, in July 2023, cybersecurity experts uncovered WormGPT, a new AI malware device that is being promoted on dark web platforms as a BlackHat Substitute for ChatGPT.[17]

   Additionally, AI is altering the way of producing and distributing malware by attackers, which renders it more hazardous and challenging to identify. This latest kind of malware, referred to as AI-driven malware, outsmarts conventional safety standards by utilising cutting-edge technologies.[18]

   AI is facilitating the production and growth of malware, and malicious individuals are on the verge to swiftly produce and distribute self-adapting mower that can get beyond various protection measures and standardised YARA verification rules.[19]

2. Identity Theft

   This particular kind of fraud has historically entailed stealing an individual's personal details in order to fraudulently pose as them, usually with an evil intention to illicitly obtain money. To acquire the required facts, cyber scammers' have employed strategies including social hacking, phishing and data infringement, which involve tricking people into divulging confidential details. But with the introduction of AI programming,

[16] Callie Guenther, *Five AI-Based Threats Security Pros Need to Understand,* SC MEDIA (October 24, 2025, 8:30 PM) https://www.scmagazine.com/perspective/five-ai-based-threats-security-pros-need-to-understand
[17] See Guenther *Five AI-Based Threats*
[18] THE CYBER EXPRESSED, *AI: cybercriminals' unlikely Best Friend*, THE CYBER EXPRESSED, (accessed October 24, 2025) https://thecyberexpress.com/evolution-of-ai-powered-cybercrime/.
[19] THE HACKERNEWS. *From Deepfakes to Malware: AI's Expanding Role in Cyber Attacks,* THE HACKERNEWS (accessed October 24, 2025) https://thehackernews.com/2024/03/from-deepfakes-to-malware-AI's-expanding.html.

ISSN: 2582-6433

identity theft has undergone changes dramatically. Further sophisticated and ubiquitous ways to conduct such criminal activities are now made possible by AI mechanisms.

A notable illustration is deepfake technological system. To enable perpetrating financial deceit or spread deceptive information, scammers use deepfakes to pose as people, especially well-known recipient to attack. Even people with little technical expertise can trick verification protocols by creating appeasing impersonations, phishing facts, and automated algorithmic data using generative AI appliances like ChatGPT, Midjourney and ElevenLabs.[20]

Synthetic identity deception cases have increased as a result of the use of AI digitalism, in which false profiles are created by combining actual and fake confidential identities. Such kind of misconducts currently accounts for 85% of all instances of identity theft, which has increased by 47% in the year 2023, and could cost US investors $ 3.1 billion in deficits.[21]

3. Market influencing

Intentional attempts to obstruct the impartial and equitable functioning of the economic sector are known as market controlling, and they frequently result in inaccurate or misleading displays on the public's demand or price of assets. The technology of AI has increased the utilisation of conventional strategies of market controlling and brought in different, more complex, and challenging-to-detect tactics.

Certain instances of AI influenced market include spoofing, which simulates demand by arranging big orders without any intention of executing them. Another instance includes schemes named pump and dump, in which automated algorithms functions by elevating stock values by creating massive numbers of purchase orders.[22] Additionally, AI is being utilised to disseminate false information by using sentiment analytical tool to artificially influence market sentiment by searching news websites and social media.[23]

[20] TRANSMIT SECURITY, *How Fraudsters Leverage AI and Deepfakes for Identity fraud*? TRANSMIT SECURITY (accessed October 25, 2025) https://transmitsecurity.com/blog/how-fraudsters-leverage-AI-and-deepfakes-for-identity-fraud.

[21] HELP NET SECURITY, *Fighting AI-Powered Synthetic ID Fraud with AI.* HELP NET SECURITY, (July 18, 2024) (accessed October 25, 2025) https://www.helpnetsecurity.com/2024/07/18/AI-powered-synthetic-identity-fraud/.

[22] Anirudh Dhawan and Talis J.Putnin, *A New Wolf in Town? , Pump-and-Dump Manipulation in Cryptocurrency Markets,* ALPHA ARCHITECT. September 2023, (accessed October 25, 2025) https://alphaarchitect.com/2023/09/a-new-wolf-in-town-pump-and-dump-manipulation-in-cryptocurrency-markets/.

[23] GLOIFY, *How AI is Untangling Stock Market Manipulation on the Web?* GLOIFY (last visited Oct. 25, 2025) https://www.gloify.com/blog/how-AI-is-untangling-stock-market-manipulation-on-the-web/.

ISSN: 2582-6433

Lawmakers and financial entities are becoming increasingly concerned about the abuse of AI in market influencing. This effect is demonstrated by empirical studies, which shows that AI-generated speculation strategies in bitcoin markets cause substantial price fluctuations and unusual trade transactions.[24]

4. Sextortion:

This specific offence is a type of blackmail in which offenders threaten to make graphic content public until and unless the targeted person agrees to fulfil their demands. With the advent of AI this crime has undergone major changes. The crime historically involved using deceptive methods or Trojan horses to get intimate photographs or recordings. However, using non-graphic photographs and video content from online networking sites or video chats, the software named deepfake allows for the production of extremely lifelike but phony sexual photos and movies.[25]

An exacerbating psychological and sentimental distress is faced by the victims because they find it difficult to demonstrate that the uploaded content is fraudulent and it needs to be taken down from the internet.

Wrong doers utilise the technology of AI to turn innocent images into obscene stuff, which re ultimately used to create a pressure upon the sufferers for monetary or any other kinds of demands. The FBI has received over 13000 reports of digital extortion of minors related to finances within a span of nearly 1.5 (October 2021 to March 2023), indicating marked rise in these occurrences. [26]Since AI-generated threats are extremely realistic, extortion is getting much more widespread and effective.

Sextortion powered by AI has serious and wide-ranging effects. Apparently 12,600 recipients, mostly boys were impacted by sextortion fraud within a period of October 2021 to March 2023, which resulted in at least 20 suicides.[27]

From 2021 to 2023, the National Center for Missing and Exploited Children (NCMEC) received over 300% numerous instances about internet enticement, including an

[24] Anirudh Dhawan and Talis J. Putnin*, A New Wolf in Town? , Pump-and-Dump Manipulation in Crypto currency Markets.* ALPHA ARCHITECT. September 2023 (Oct 25, 2025) , https://alphaarchitect.com/2023/09/a-new-wolf-in-town-pump-and-dump-manipulation-in-cryptocurrency-markets/.

[25] FBI, *Sextortion: A Growing Threat Preying Upon Our Nation's Teens* (accessed October 26, 2025.) https://www.fbi.gov/contact-us/field-offices/sacrmento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens.

[26] Ibid

[27] FBI, *Sextortion: A Growing Threat Targeting Minors.* (accessed October 26, 2025). https://www.fbi.gov/contact-us/field-offices/memphis/news/sextortion-a-growing-threat-targeting-minors.

ISSN: 2582-6433

ongoing rise in financial sextortion claims.[28]

5. Use of AI in cyber terrorism:

One of the primary strategies used by terrorist organizations to spread their ideals and concepts is propaganda. This might turn out to be more effective and target-specific with the id of generative AI, which would also make it easier to disseminate and have a significant influence. The use of fabricated images, video or audio content that re consistent with the organization's values could strengthen texts, broaden the scope of propaganda, and influence public reactions and thoughts (For instance, using synthetic photos of injured victims or any vulnerable groups to have an emotional effect on the viewers.)

Since certain contents on online platforms can be swiftly shared by millions of followers, therefore, there prevail high chances that specific AI-generated content may be used to expand the audience and propagate misinformation.

The ongoing conflict in Gaza serves as a relevant instance of how terrorist have employed generative AI to encourage further aggression and spread misinformation through several photographs that has been published online. With the help of generative AI, images of infants or young kids harmed in the conflict seemed to have been altered to add extra turmoil and unsettling facts at the world web.

CHAPTER-9: SUGGESTIONS AND RECOMMENDATIONS

1) **Enforcement of specific provisions for AI**: An enactment of AI specific laws must be made in order to regulate the various algorithms associated for proper operation of AI bringing transparency and data analysis powered by AI in alignment with international norms.
2) **Implementation of consensual data collection**: An approach must be established introducing free will to provide and revoke consent by the individuals, to ensure users are fully aware and have a clear understanding of the techniques to be used by AI for processing their personal data.
3) **Enactment of right to interpretation**: A method must be initiated to ensure maintenance of accountability and transparency by legally requiring AI systems to interpret automated decisions that affect users.

[28] Jacob Knutson, *How AI is Helping Scammers Target Victims in 'Sextortion' Schemes*? AXIOS, June 23, 2023, (accessed October 26, 2025), https://www.axios.com/2023/06/23/artificial-intelligence-sexual-exploitation-children-technology.

ISSN: 2582-6433

4) **Regulations restricting AI surveillance**: Definitive strict barriers should be made on surveillance of data driven by AI technologies, such as facial identification and search engine operation, to prevent massive surveillance and privacy breaches.
5) **Liability norms for various AI organisations**: There should be liability rules for any kind of data infringements conducted by AI systems, which needs to be abided by various associations, developers, organisations and various government executives, to protect privacy.
6) **Removal of biasness and inauguration of ethics while operating AI mechanisms**: Making of rules mandating regular AI audits for proper algorithm recognition and removal of any biased practices, by conducting AI applications to operate in a non-discriminatory manner.
7) **Public awareness and knowledge about digitalism:** Measures for promoting AI awareness must be adopted through campaigns to propagate AI techniques and to uphold data privacy. Such measures should be taken to educate citizens' about their rights and methods to safeguard their personal information from risks.
8) **Worldwide agencies collaboration:** An alignment must be initiated between India's AI provisions and worldwide best AI processing developments which includes European Union GDPR and OECD AI principles, in order to protect massive outflow of data cross-border from any illegal use and ethical data analysis by AI mechanisms.
9) **Artificial Intelligence and data protection rights:**
   a) **Right to information and access:** People can acquire information regarding what data an organisation is collecting, how it is collecting it, how it will utilise it, and if automated decisions are generated from these data, credit shall be showered upon the combined rights of right to information and access.

   These rights raise consciousness among public and operational functions of AI systems are also made more widely known through these rights[29]. They also enable people to identify and comprehend possible violations of human rights and hold organisations accountable for their use of AI.

   b) **Right to rectification:** If a third party holds imprecise, partial or incorrect information about a person, the concerned person carries the right to update nod alter it. This privilege can lessen the effect of AI systems' error rates.

[29] *In the US, many of the details of government use of algorithmic decision making system are hidden behind non-disclosure agreements and memorandums of understanding with vendors*. See https://www.wired.com/story/when-government-rules-by-software-citizens-are-left-in-the-dark/.

ISSN: 2582-6433

c) **Right to limitation in data processing:** Users have the right to appeal that an entity ceases using or restrict the use of their personal details. However, when personal data is no longer required and has been mishandled, or their relationship with third party business ends, they have the right to have it deleted through the right to erasure. The contentious AI system could be temporarily restricted or n entity could be pressured to utilise an AI mechanism with greater integrity by employing these rights.

d) **Right to interpretation or explanation:** According to the right to interpretation, n individual has the right to acknowledge how an algorithmic choice concerning them is made. This right encourages AI developers to keep endeavouring to generate AI more comprehensible and guarantees that entities re conscious of concerning the way the technology they deploy truly operate.

e) **Right to raise objection:** This right permits individuals to confront an overwhelming majority of how an entity processes their personal data when it is used for statistical analysis, computerised decision-making (in which no participation of man is required), commercial purposes, or n entity's "legitimate enthusiasm"

Direct disagreements to judgments made by AI applications are made possible by this right. The employment of AI by the government in potentially prejudiced practices is very crucial. Additionally it guarantees that a human is involved in crucial automated decision-making process, which raises the bar for responsibility.

CONCLUSION

The inter-relationship between data privacy and artificial intelligence poses vital ethical and legal issues that need to be resolved for responsible and appropriate application of AI technologies. When AI systems are developed and implemented organizations are required to adhere to certain significant principles like being transparent, accountable, acquiring user's consent, being fair, establishing secured connectivity, reduction in data collection and user control.

Organizations are required to comply with the framework provided by current privacy rules and directives such as GDPR and CCPA, but ongoing efforts required to adjust to the changing landscape of data management and AI appliances.

Governing authorities are established so that they could keep a check and enforce compliance with the privacy regulations pertaining to AI. Addressing the ethical issues of data privacy in

ISSN: 2582-6433

the context of artificial intelligence required cooperation between regulatory bodies, industrial players, academic institutions and various other stakeholders.

The paper also focus on various crimes committed with the advent of AI, showcasing although AI technology has many positive aspects, it also possess certain deadly risks and unfavourable repercussions as digital attackers are upgrading their ways of malicious attacks t constant pace. Therefore, AI is like a double-barrelled weapon that requires a legal sheath. It is anticipated that the use of this emerging invention, which entails the ability to make decisions on its own, would constitute legal ramifications. The current justice framework is inadequate to address the emerging online illicit activities that are facilitated by AI. With due regard to all these facts, for the administration of the judiciary to successfully combat cybercrimes, proper AI legislation strategizing AI is sorely desired.

In conclusion, the government my play a significant role in establishing a framework that balances technological advancement with a dedication to built reliable and equitable AI. Since, exorbitant, unsuitable or misguided legislations my hinder the widespread implementation of AI or fail to effectively tackle its real difficulties, striking the correct equilibrium requires a cooperative, multidisciplinary strategy. The development, application and regulation of AI will heavily rely on rethinking conventional ideas and utilising current information of privacy policies.

REFERENCES

1) The Committee of Experts on Internet Intermediaries; Algorithms *and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, COUNCIL OF EUROPE, 10-12, March (2018), https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5
2) Robert Brauneis and Ellen P. Goodman, *Algorithm transparency for the smart city*, 20 THE YALE JOURNAL OF LAW AND TECHNOLOGY, 103-176 (2018)
3) Steven M Bellovin, et al, *When enough is enough: Location tracking mosaic theory, and machine learning,* NYC JOURNAL OF LAW AND LIBERTY, 555-628 (2014)
4) FREEDOM HOUSE SURVEY FOUND 30 OF 65 OF GOVERNMENTS ATTEMPTED TO CONTROL ONLINE DISCUSSIONS. https://freedomhouse.org/article/new-report-freedom-net-2017-manipulting-social-media-undermine-democracy
5) *Germany starts enforcing the speech law*, THE BBC, January 1,2018, https://www.bbc.com/news/technology-42510868

ISSN: 2582-6433

6) Privacy International and Article 19, *Privacy and Freedom of Expression in the Age of Artificial Intelligence,* April 2018 (September 30, 2025, 4:30 PM), https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-rtificil-Intelligence-1.pdf.

7) Nick Lawrence, *AI in UI, 2323 and Beyond*, MEDIUM (28th August, 2024)(last visited Oct 29, 2025), https://uxplanet.org/ai.in.ui-2023-and-beyond-346b4602eff7

8) Dr. Mark Van Rigmenam, *Privacy in the age of AI risk, challenges and solution,* www.digitlspeker.com (22 August 2024)

9) Yancy Dennis, *Artificial Intelligence- privacy and ethics,* MEDIUM (28th August 2024) (last visited Oct 29, 2025), www.medum.com

10) Alexandra Jonker & Julie Rogers. *What is algorithmic bias?* IBM (Oct. 28, 2025, 3:47 PM), https://www.ibm.com/think/topics/algorithmic-bias

11) Vera Lucia Raposo, *How is 'Unexplainable' and Non-transparent AI affecting Healthcare Delivery?*, 11 SPECIAL ISSUE: AI AND ROBOTICS IN HEALTHCARE SCIENTIFIC PUBLICATION, 1, 2-8 (2024)

12) *The Rise of AI-Enabled Crime: Exploring the Evolution, Risks, and Responses to AI-powered Criminal Enterprises*, TRM BLOGS (Jan 29, 2025) (last visited Oct 28, 2025) https://www.trmlabs.com/resources/blog/the-rise-of-ai-enabled-crime-exploring-the-evolution-risks-and-responses-to-ai-powered-criminal-enterprises

13) Callie Guenther, *Five AI-Based Threats Security Pros Need to Understand,* SC MEDIA (October 24, 2025, 8:30 PM) https://www.scmagazine.com/perspective/five-ai-based-threats-security-pros-need-to-understand

14) THE CYBER EXPRESSED, *AI: cybercriminals' unlikely Best Friend*, THE CYBER EXPRESSED, (accessed October 24, 2025) https://thecyberexpress.com/evolution-of-ai-powered-cybercrime/.

15) THE HACKERNEWS. *From Deepfakes to Malware: AI's Expanding Role in Cyber Attacks,* THE HACKERNEWS (accessed October 24, 2025) https://thehackernews.com/2024/03/from-deepfakes-to-malware-AI's-expanding.html

16) TRANSMIT SECURITY, *How Fraudsters Leverage AI and Deepfakes for Identity fraud*? TRANSMIT SECURITY (accessed October 25, 2025) https://transmitsecurity.com/blog/how-fraudsters-leverage-AI-and-deepfakes-for-identity-fraud.

ISSN: 2582-6433

17) HELP NET SECURITY, *Fighting AI-Powered Synthetic ID Fraud with AI.* HELP NET SECURITY, (July 18, 2024) (accessed October 25, 2025) https://www.helpnetsecurity.com/2024/07/18/AI-powered-synthetic-identity-fraud/.

18) Anirudh Dhawan and Talis J.Putnin, *A New Wolf in Town?, Pump-and-Dump Manipulation in Cryptocurrency Markets,* ALPHA ARCHITECT. September 2023, (accessed October 25, 2025) https://alphaarchitect.com/2023/09/a-new-wolf-in-town-pump-and-dump-manipulation-in-cryptocurrency-markets/.

19) GLOIFY, *How AI is Untangling Stock Market Manipulation on the Web?* GLOIFY https://www.gloify.com/blog/how-AI-is-untangling-stock-market-manipulation-on-the-web/.

20) FBI, *Sextortion: A Growing Threat Preying Upon Our Nation's Teens* (accessed October 26, 2025.) https://www.fbi.gov/contact-us/field-offices/sacrmento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens.

21) Angwin et al, *Machine Bias,* https://www.scirp.org/reference/referencespapers?referenceid=3337609

22) Jacob Knutson, *How AI is Helping Scammers Target Victims in 'Sextortion' Schemes*? AXIOS, June 23, 2023, (accessed October 26, 2025), https://www.axios.com/2023/06/23/artificial-intelligence-sexual-exploitation-children-technology.

23) *In the US, many of the details of government use of algorithmic decision making system are hidden behind non-disclosure agreements and memorandums of understanding with vendors*. See https://www.wired.com/story/when-government-rules-by-software-citizens-are-left-in-the-dark/.