THE IMPACT OF ARTIFICIAL INTELLIGENCE ON PRIVACY RIGHTS IN INDIA

Saniya Ansar & Mohd. Anas, B.A. LL.B. (5 Year Integrated), School of Law, Hamdard Institute of Legal Studies & Research (HILSR), Jamia Hamdard

LIST OF ABBREVIATIONS

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
FRT	Facial Recognition Technology
EU	European Union
GDPR	General Data Protection Regulation
DPDP	Digital Personal Data Protection
IT	Information Technology
UAE	United Arab Emirates
IBM	International Business Machine Corporation
GANS	Generative Adversarial Network
GPT	Generative Pre-Trained Transformer
CCTV	Close Circuit Television
IOT	Internet Of Thing
ROI	Return Of Investment
FTC	Federal Trade Commission
NIST	National Institute of Standard Technology
CCPA	California Consumer Protection Act
R&D	Research And Development
ART.	Article

US	United Stated
UK	United Kingdom
NITI	National Institutional of Transforming India
RBI	Reserve Bank of India
ICMR	Indian Council of Medical Research
UOI	Union Of India
VS.	Versus

CHAPTER – 1

INTRODUCTION

Artificial intelligence (here in after referred as AI), essentially refers to the stimulus of human brains in machines. These can learn to solve problems, recognize patterns, and make decisions. Also, AI powers technologies like chatbots, voice assistants, facial recognition, and selfdriving cars. It is extensively used in industries such as healthcare, finance, and education to improve effectiveness and correctness. The AI systems operate data to function. They process huge amounts of individual information to make improved decisions in areas like healthcare, finance, education, and governance. We see AI improving accessibility and competence in many ways, from facial recognition at airports to AI-powered customer service bots. But this substantial dependence on data also brings serious privacy dangers. The absence of strict data protection laws makes it easier for authorities to track citizens without clear legal oversight, and this is risky in our daily lives. We, the residents of India, are facing such problems in the arena of facial recognition. It is observed that there is growing use of facial recognition technology (FRT). While it helps in crime deterrence, it also raises alarms about mass surveillance and probable misuse of data. This is the first concern, and the other is data collection. Without consent, for example, many AI-driven applications collect personal data without users' informed consent. Whether through social media mobile apps or government databases, individuals often do not know how their data is being used or shared, and this lack of transparency is likely to be a direct threat to the right to privacy, which was upheld as a fundamental right by the Supreme Court of India in the *Puttaswamy judgment of 2017*[1]. This

[1] K.S. Puttaswamy v. Union of India [2017} 10 SCC 1

decision significantly influenced discussions on AI governance and data protection. However, concerns remain about AI-driven government surveillance—such as Aadhaar's biometric identification system—and private companies collecting and processing vast amounts of personal data.

India urgently needs strong data protection laws to control how AI affects privacy. The Digital Personal Data Protection, Act 2023 is a step in the right direction, but it must be enforced properly so that it gives individuals stronger data and privacy rights, sets clear rules for AI-based data collection and use, and imposes strict penalties for misusing personal data. These cybersecurity threats can't be unseen as AI-driven cyberattacks can misuse personal data, causing identity theft, financial fraud, and leaks of sensitive information. As India rapidly embraces digital technology, these cyber threats are creating some major challenges in protecting privacy. In this research, we're going to find all these impacts and see the things and mishaps caused, plus what should actually be done for protection and that the basic role of the laws made on data protection is regulating AI's impact on our privacy.

LITERATURE REVIEW

In the case of Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017)[2]

In the 2017 case of Justice K S Puttaswamy, the Supreme Court of India held that the right to privacy is a constitutional right. The landmark decision overturned two previous judgments and raised concerns about the proposed biometric data collection scheme. The court held that privacy covered both personal and informational aspects of the case but could be restricted for reasons of good governance. The judgment brought about a major overhaul of privacy laws in India and shaped debates around data protection and surveillance, and may also shape future data protection laws.

Artificial Intelligence: Impact on Right to Privacy [3]

The article explores the growing privacy risks associated with AI such as surveillance/data breaches/biased profiling/misuse of personal data without consent. It highlights the need for strong data protection laws in our country citing the EU's General Data Protection Regulation

[2] Supra note 1 pg 1
[3] Kashish Maggo, "Artificial Intelligence: Impact on Right to Privacy", Juris Centre, [12 September 2023] , available at[https://juriscentre.com/2023/09/12/artificial-intelligence-impact-on-right-toprivacy/]

as a prime example of this concern that we have implemented. In our nation where privacy is a fundamental right, AI-driven technologies such as facial recognition and data analytics raise significant concerns in many ways that are always likely to pose a threat to our lives. In the Indian context, the article discusses the constitutional right to privacy and its impact on data protection laws. It points out that technologies such as surveillance cameras, facial recognition, data analytics, and AI can erode privacy by collecting and analysing vast amounts of personal data. Balancing technological benefits with privacy protection is crucial in the digital age. The article advises a balanced approach that protects privacy while promoting innovation, emphasizing the urgent need for comprehensive legal protection in an AI-driven world. Too often, it is about deceiving each other, which is never an ethical imperative for our society.

A Study on the Impact of Artificial Intelligence on the Right to Privacy in India [4]

AI is transforming industries such as healthcare and finance, but it also raises serious privacy issues. This article examines the conflict between the growth of AI and security, particularly after India's 2017 Puttaswamy ruling, which recognized privacy as a fundamental right. With AI increasingly dependent on personal data, strengthening data protection laws is crucial to protecting our information from breaches. The paper examines how technologies such as facial recognition and predictive policing could escalate surveillance and privacy violations. AI's ability to make decisions based on data patterns without human oversight poses risks that current regulations do not adequately cover. The paper focuses primarily on India's data protection framework, particularly the ongoing debate around the Digital Personal Data Protection Act, 2023. The paper criticizes the bill for failing to address issues related to AI, such as AI-generated data and inadequate regulatory measures to monitor AI. By contrast, the General Data Protection Act provides stronger protection against misuse of AI, while India's laws do not adequately address the unique privacy risks of AI. Furthermore, the authors will discuss the ethical implications of AI, emphasizing the need for a robust ethical framework to guide its development and use. Without such a framework, AI could perpetuate bias, violate privacy, and disproportionately impact marginalized communities.

[4] Rohith S B & Sethupriya N, "A Study On Impact Of Artificial Intelligence On Right To Privacy In India", Indian Journal Of Legal Review, 2024

Impact of Artificial Intelligence on Privacy Harms: A Taxonomy Of Intrusion & Privacy Risk Assessment Framework, 2024[5]

The paper examines the multifaceted challenges AI presents to personal privacy. As AI technologies evolve quickly, they are being applied across industries like healthcare, finance, and law enforcement, with uses ranging from facial recognition to predictive analytics. Although these advancements bring substantial advantages, they also introduce notable privacy risks that need to be carefully assessed and regulated. A key strength of this paper is its development of a taxonomy of AI-induced privacy harms, which categorizes different forms of privacy harms based on their nature and severity. This framework helps to better understand the specific ways in which AI technologies can violate individual privacy, from direct surveillance and data collection to more subtle forms of data profiling and algorithmic decision making. By categorizing privacy risks into distinct categories, the paper provides a nuanced perspective on how AI-driven systems impact individuals' rights to privacy, autonomy, and personal security.

Furthermore, the paper proposes a privacy risk assessment framework that aims to assess the potential harms posed by AI systems in different contexts. This framework is valuable because it provides a structured approach to identifying, assessing, and mitigating privacy risks associated with the deployment of AI technologies. It emphasizes the need for transparency, accountability, and ethical considerations in AI development to ensure that privacy harms are minimized and individuals' rights are protected. The authors also emphasize the importance of developing legal and regulatory mechanisms to address these privacy concerns. The paper suggests that current legal frameworks, such as India's draft Personal Data Protection Bill, may not be fully equipped to address the complexities of AI, and that further reforms are needed to protect individuals in an AI-powered future.

Emergence of AI and Its Implication Towards Data Privacy: From an Indian Legal Perspective[6]

The paper sheds light on the growing nexus between AI and data privacy in India. The paper

[5] Avinash Dadhich & Vasanthika Srinath , "Impact of Artificial Intelligence on Privacy Harms: A Taxonomy of Intrusion & Privacy Risk Assessment Framework"[2024] [published Master of Laws (LL.M.) dissertation, Manipal Law School MAHE, Bengaluru]

[6] D. Majumdar and H.K. Chattopadhyay, "Emergence of AI and its Implication Towards Data Privacy: From Indian Legal Perspective" 3 International Journal of Law Management & Humanities 1-20 (2020).

provides a critical examination of the ways in which AI systems, which rely on large amounts of data, can threaten people's right to privacy. The article highlights the challenges posed by the development of AI in Indian legal language, particularly in the current data protection laws.

The authors examine the potential risks to people's personal information posed by the increasing use of AI and the lack of robust privacy rules. The paper makes a significant contribution to the discourse on balancing privacy protection with technological innovation, and calls for the creation of a data protection framework that addresses the evolving nature of AI in India.

Privacy in context: Technology, Policy, and the Integrity of Social Life[7]

This book offers a comprehensive examination of privacy that emphasizes its relational role and goes beyond traditional views of privacy or data control. According to Nissenbaum, privacy should be viewed as the ability to regulate the transfer of private information in particular social contexts, where people may expect their information to be shared in certain ways based on the situation. This approach, called contextual theory, contrasts with traditional privacy frameworks that emphasize personal freedom and control. In the digital age, where technology is constantly changing how personal information is shared and used across different platforms, Nissenbaum's work is particularly relevant. The book convincingly challenges current privacy laws, which often fail to adequately protect people in context, and calls on policymakers to take action.

STATEMENT OF PROBLEM

As AI technology advances and becomes more integrated, there are significant concerns about the potential erosion of privacy rights in India. AI systems use large amounts of personal data, which is frequently collected, analyzed, and evaluated in ways that individuals may not fully understand or agree to. Unfettered use of AI could violate people's right to privacy in India, where privacy is protected by the Constitution as a fundamental right. This is because the technology could enable unintended surveillance, targeting, and misuse of personal data. Despite strong data protection legislation such as the Digital Personal Data Protection Act,

[7] Helen Nissenbaum, Privacy in Context Technology, Policy, and the Integrity of Social Life (Stanford University Press, Stanford, California, 2009).

2023, there remains a significant gap in addressing the complex privacy challenges posed by AI. Therefore, the problem description underscores the need to consider how AI technologies impact people's privacy rights in India, especially in the context of exponentially increasing technological innovations in data access, licensing, accountability, and existing regulations to protect people's private data.

RESEARCH QUESTION

1. What are the key privacy concerns arising from the deployment of AI technologies in India?

2. What is the role of data protection laws, such as the Digital Personal Data Protection Act, 2023 in regulating AI's impact on privacy?

3. In what ways can AI be utilized to strengthen privacy rights rather than infringe upon them?

PURPOSE OF STUDY

This research looks at how the AI impacts privacy rights in India, focusing on the legal, ethical, and technological aspects. Our study examines current data prevention laws like the Personal Data Protection Act 2023, the Information Technology Act 2000, etc., to see how well these are addressing AI-related issues of privacy. The study also explores AI-driven surveillance, data collection, and automated decision-making, analysing their effects on individual privacy and fundamental rights under the Indian Constitution. Plus, reviews on the courts rulings and regulating policies suggest ways to balance out AI advancements with strong privacy protections in our nation. The purpose of this research is to identify challenges faced by individuals related to privacy in an AI-driven society and suggest potential measures and safeguards and recommend best practices to improve privacy protection in the context of AI.

HYPOTHESIS

The increasing deployment of Artificial Intelligence (AI) technologies in India poses significant challenges to privacy rights due to inadequate regulatory frameworks.

METHODOLOGY

The research shall be doctrinal. It will include both the primary and secondary sources available on the subject. Among the primary sources, the study shall focus on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and the Digital Personal Data Protection Act, 2023, etc. The research shall review court judgments or legal opinions related to AI. Under secondary sources, books, research papers, and articles on the subject will be discussed in detail to understand the problem in depth.

CHAPTER – 2

UNDERSTANDING ARTIFICIAL INTELLIGENCE AND PRIVACY

Artificial Intelligence (AI) refers to machines' ability of learning and responding like humans. The demand for AI is growing rapidly day by day and significantly it is impacting on technology and business. Countries like the UAE are preparing for the AI revolution by appointing leaders such as Omar Sultan Al Olama as Minister of AI[8]. As AI expands into nearly every area of life, it is bringing challenges related to privacy, safety, employment, and intellectual property to us in every way.

Concept of Artificial Intelligence

Firstly, we need an Understanding of what AI truly is now and how it can be challenging, as the term has evolved over time. Traditionally, AI was associated with sentient robots, but today it basically refers to machine learning algorithms and related technologies, which differ from machines which can think independently. AI is far more complex nowadays and more powerful than just another technology. As AI expert Mustafa Suleyman explains that the real risk lies not in exaggerating its impact but in underestimating the magnitude of the coming wave—AI is not just a simple tool or platform but it is a transformative meta technology which can be dangerous to our society in many ways.[9]

Early definitions of Artificial Intelligence were focused solely on a replicating intelligence at

[8] Billy Perrigo**,** "The UAE Is on a Mission to Become an AI Power"**,** Time, March 20 ,2024.
[9] Daniel J. Solove, "Artificial Intelligence and Privacy",77 Florida Law Review 7(2025)

a mechanical level.

The first definition was given by John McCarthy from Stanford University, who coined the term in 1956. He defined AI as "the science and engineering of making intelligent machines".[10] The field was established on the belief that human intelligence could be described precisely enough to be simulated by a machine.

Whereas Nilsson defined AI as "That activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment."[11] AI is about developing intelligent machines that act smart, not simply reacting to things, but thinking forward and making excellent decisions depending on their surroundings.

Stuart Russell and Peter Norvig defined AI as "the study of agents that receive percepts from the environment and perform actions[12]. According to this definition, artificial intelligence is defined in terms of intelligent agents, which are systems that use inputs known as percepts to observe their environment and then react by acting in ways that advance their objectives[13]. Here, the emphasis is on how successfully an agent behaves in its surroundings based on its perceptions, not merely on thinking or learning. According to the theory, an agent's ability to make judgments and adjust to new knowledge in order to solve issues or finish tasks is a good indicator of their intelligence. This method is practical and goal-oriented, emphasizing behavior and contact with the real world.

Kaplan and Haenlein defined AI as "A system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation"[14].

Patrick Mikalef and Manjul Gupta says "AI is the ability of a system to identify, interpret, make inferences, and learn from data to achieve predetermined organizational and societal

[10] Prof Dalvinder Singh Grewal, "A Critical Conceptual Analysis of Definitions of Artificial Intelligence as Applicable to Computer Engineering",16 IOSR Journal of Computer Engineering 10 (2014)
[11] Stanford University," Artificial Intelligence and Life in 2030: The One Hundred Year Study on Artificial Intelligence(AI100)"12(2016).
[12] Stuart Russell and Peter Norvig," Artificial Intelligence A Modern Approach", Pearson Series In Artificial Intelligence 54,2022
[13] Ibid 12
[14] Andreas Kaplan and Michael Haenlein,"Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence", 62 Business Horizons 15 ,2019

goals[15].” All the definition makes AI’s focus on mimicking human learning mechanisms, processing information, and coping with conditions that need problem solving.

AI systems are typically classified into levels depending on their intelligence and capabilities. Narrow AI, also known as Weak AI, is meant to do specialized tasks like facial recognition or language translation. General AI, also known as Strong AI, has human-level intelligence and can carry out any intellectual work that a human can. While an ambitious objective, General AI remains essentially a theoretical concept. Finally, Super AI conceptually outperforms human intelligence in all categories while remaining firmly in the realm of a theory.[16]

Mona Ashok and Rohit Madan defined AI as machines or "assemblage of technological components" that perform cognitive functions associated with human minds, operate autonomously without human intervention, and learn and identify patterns to make decisions. The framework of their definition consists of four domains: physical, cognitive, information, and governance, which are used to map digital ethics implications and AI concepts.[17] The physical domain includes implications related to dignity and well-being, safety, and sustainability. The cognitive domain includes implications related to intelligibility, accountability, fairness, promoting prosperity, solidarity, and autonomy. The information domain includes implications related to privacy and security. The governance domain includes implications related to regulatory, financial and economic, and individual and societal impact.

Historical Timeline

In 1950, British mathematician and computer scientist Alan Turing published a in which he posed the famous question, “Can machines think?” and proposed a turing test to examine a machine's ability to exhibit intelligent behaviour equivalent to, or indistinguishable from, that of a human[18]. This is considered as birth of AI. After this in 1966 ELIZA Chatbot Developed as one of the first AI programs to simulate human conversation by computer scientist Joseph Weizenbaum , and was intended to simulate therapy by repurposing the answers users gave into questions that prompted further conversation(also known as the Rogerian argument) ,

[15] Patrick Mikalef and Manjul Gupta,” Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance,58 Information and Management , 2021
[16] Vijay Kanade,” Narrow AI vs. General AI vs. Super AI: Key Comparisons”, Spiceworks, 2022
[17] Mona Ashok; Rohit Madan; Anton Joha et al,” Ethical framework for Artificial Intelligence and Digital technologies”, Queens University Belfast, 2021
[18] A. M. Turing, “Computing Machinery And Intelligence”, 59 Mind, 1950

This was one of the first AI chatbots, mimicking a therapist by turning user statements into reflective questions.[19] The Artificial Intelligence Centre at the Stanford Research Initiative developed Shakey the Robot in 1970s, a mobile robot system equipped with sensors and a TV camera which it used to navigate the different environments at different time. While Shakey's abilities were rather crude as compared to today's developments in this sector, the robot helped advanced elements in AI by including a "visual analysis, route finding and the object rearrangement[20]. After few years the phase of first AI winter occurred in the field of artificial intelligence from 1974 and 1980. During this time, funding, public interest, and excitement for AI research all significantly decreased. This decline was mostly brought on by governments' and funding organizations' mounting dissatisfaction with the slow pace of development and minimal practical uses of AI systems at the time.[21] After passing of AI Winter phase , IBM's Deep Blue a chess-playing computer program beats Garry Kasparov Demonstrated the actual power of AI by defeating the world chess champion in 1997. Deep Blue didn't have the functionality of today's generative AI, but it could process information at a rate which is far faster than the human brain. In one second, it could review 200 million potential chess moves which a normal brain can't afford at any cost. [22] Many years after IBM's Deep Blue program successfully beat the world chess champion, the company created another competitive computer system in 2011 which would go to play the hit US quiz show Jeopardy. In the leadup to its debut, Watson DeepQA was fed data from encyclopedias and across the internet. Highlighted AI's capabilities in natural language understanding and answering all the complex queries without any lack in between. This was a unbelievable response at that time which can't be neglected at all[23]. Generative Adversarial Networks (GANs) was introduced in 2014. This Revolutionized AI by enabling machines to create realistic data like images and videos this was fictional at that time but when it happened it shocked everyone at that time and this was the first time when people realised ai was a threat to peoples jobs[24].In 2016, an artificial intelligence program AlphaGO created by the AI research lab Google DeepMind, went on to beat Lee Sedol, one of the best players in the world. AlphaGO is a combination of

[19] Manisha Salecha," Story of ELIZA, the first chatbot developed in 1966", Analytics India Magazine, October 5, 2016 available on https://analyticsindiamag.com/ai-features/story-eliza-first-chatbotdeveloped-1966/ (last visited on 10 april)
[20] Stanford. "Shakey the Robot", available at https://ai.stanford.edu/~nilsson/OnlinePubs-Nils/shakeythe-robot.pdf.
[21] Ellen Glover," What Is AI Winter?" , Builtin, 2023
[22] IBM. "Deep Blue." IBM History, available at www.ibm.com/history/deep-blue.
[23] IBM, "Watson on Jeopardy!" IBM History, available at https://www.ibm.com/history/watsonjeopardy.
[24] Macro Del Pra, "Generative Adversarial Networks." Medium, 17 Oct. 2017, available at https://medium.com/@marcodelpra/generative-adversarial-networks-dba10e1b4424.

neural networks and the advanced search algorithms which were trained to play Go using a method which is called reinforcement learning, this strengthened its abilities over the millions of games that it played against itself. When it beated Sedol, it proved that AI could tackle once undefeatable problems. This was the great peak time in the rise of AI cause after this directly the combination of all powers of AI were launched which is still growing and leading our daily lifes.[25] In 2020 OpenAI introduces GPT-3 a landmark in natural language processing, showcasing human-like text generation.{ generative pre-trained transformer (GPT) that became the architectural foundation for its early language models GPT-1 and GPT-2, which were trained on billions of inputs. . GPT-3 was trained on 175 billion parameters, which far exceeded the 1.5 billion parameters GPT-2 had been trained}[26].ChatGPT, launched by OpenAI in 2021, sparked a major AI boom with the realistic, conversational abilities far beyond earlier than chatbots. It's used for tasks like writing, coding and research. Its massive success led to a wave of similar tools and raised concerns about the AI safety and responsible use. [27]

Concept of privacy in context of AI

Privacy refers to the right of individuals to control their personal information—how it is collected, used, stored, and shared. It is a fundamental human right that protects individuals from unwanted surveillance, misuse of data, and intrusion into their personal lives [28]. In both digital and physical spaces, privacy ensures that people can express themselves, make decisions, and live without constant observation or interference

AI systems take in data which is known as (inputs) and produce results which is called the (outputs), and both can cause privacy issues[29]. These issues aren't new, but AI makes them more complicated and harder to manage. Input problems include how AI collects the data—like scraping public info from the internet or collecting it through the apps and services. Often, people don't know or fully understand that how their data is being collected and current privacy laws don't do a good job of protecting against this chase. Output problems happen when AI creates new data or makes a decision based on what it learns or already have learnt.

[25] DeepMind. "AlphaGo." Google DeepMind, available at https://deepmind.google.com/research/breakthroughs/alphago/.
[26] Rahib Imamguluyev, "The Rise of GPT-3: Implications for Natural Language Processing and Beyond",4 International Journal of Research Publication and Reviews (2023)
[27] Md Asraful Haque, "A Brief Analysis of ChatGPT – A Revolutionary Tool Designed by OpenAI", EAI Endorsed Transactions on AI and Robotics (2023)
[28] Daniel J. Solove, "Understanding Privacy", Harvard University Press, 2008
[29] Supra 9

This can reveal private information of people who didn't mean to share. It also makes it easier for companies or governments to track, analyse and control the people.

AI systems need a huge amount of data to work properly. For example, ChatGPT grew from using 1.5 billion data points to 175 billion in just a single year. This data often includes personal and sensitive information like names, photos, health records or even facial features sometimes collected without a clear consent basically by unethical ways. AI also makes it easier to automate the surveillance and identification. For example, regular CCTV cameras are one thing but adding facial recognition makes them way more powerful in many ways.

"As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed."[30]

The AI system learns from personal information like our search history, photos or even voice recordings to make some smart choices or suggestions. Because AI collects and analyzes the data about what we do, where we go and what we like, AI can accidentally share or expose these private details (for example, targeted ads seeing our recent searches). That's why keeping control of our data by limiting what we share, understanding how it's used, and choosing services with strong privacy safeguards is very essential for using AI safely and protecting our personal life. This is where AI and privacy come to a relationship in which AI is the user and privacy is the one which is getting exhausted in feeding the AI systems. Privacy denotes the right of an individual to control his/ her data collected, processed and stored by intelligent systems - it requires bound to principles such as data minimization, informed consent, anonymization, transparency and security safeguards to prevent all unauthorized access and ensure legal and ethical compliance.

CHAPTER – 3

AI FOR CRIME PREVENTION:

THE BALANCE WITH PRIVACY RIGHTS

In past few years advancements in technology have transformed the crime prevention efforts

[30] Cameron F. Kerry," Protecting privacy in an AI-driven world", Brookings, 2020

in many ways which is leading to the incorporation of artificial intelligence (AI) into law enforcement practices. AI technologies mainly as machine learning, predictive analytics and natural language processing have been deployed to the enhance crime prevention strategies.

The integration of AI in law enforcement is not only aims to improve efficiency but also seeks to enhance the public safety through data-driven decision-making. However, the deployment of AI technologies has raised many concerns about the privacy, accountability and biased judgement plus decisions. As AI continues to evolve it is very crucial for law enforcement agencies to navigate all these challenges while harnessing the main potential of AI to create safer communities.

AI IN CRME PREVENTION

In this world of modern technologies many complicated things are getting solved more accurately than before within a short duration of time with the help of these computers. This is possible only due to the recent advances in this field of computer science and technology. In many fields of science now machines and computer technologies are utilized to perform human-like tasks such as critical thinking, analysis, reasoning, planning, creativity, and the main task of decision-making to solve all the vast and complicated problems. This ability of machines & computers may be defined as Artificial Intelligence (AI). They are capable of adapting behaviour to a certain degree of limitless boundaries by analysing the effects of previous actions they or we took in life and working autonomously.

1. AI in Predictive Policing

Predictive policing is an innovative approach which basically employs all the data analysis and the statistical algorithms to anticipate and prevent all potential criminal activities. By using all the historical criminal data, geographical information and social indicators the law enforcement agencies aim to allocate resources more efficiently and intervene before crimes going to occur.[31]This method is shifting the main focus from reactive policing (responding to crimes after they have happened) to proactive strategies which aimed at the deterring criminal activities. Predictive policing techniques can generally be divided into four main types: those that forecast where crimes are likely to occur, those that anticipate who might commit a crime,

[31] Walter L. Perry, Brian McInnis, Carter C. Price, Susan Smith, John S. Hollywood.et.al," Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations", Rand 1,2(2013)

those that aim to identify potential suspects, and those that predict who may become a victim of a crime.[32] Crime prediction tools now use not just past crime data but also the social behavior information—like data from friends' and family members' social media, as well as the economic and community details of persons and societies. This extra data basically helps these tools to check how social and economic factors connect to crime so that police can spot all the high-risk areas. This allows the law enforcement to focus on their efforts and resources more efficiently so they can stop the crimes before they happen in real life.

Chicago has also seen positive outcomes from predictive policing initiatives. The Chicago Police Department utilizes a predictive analytics program called "HunchLab." This system integrates various data sources, including crime reports, socio-economic data, and environmental factors, to forecast crime likelihood. A study by the University of Chicago Crime Lab found that neighbourhoods using HunchLab experienced a 12% decrease in shootings over a two-year period compared to similar areas not using the system .The success of this initiative underscores the potential for data-driven strategies to mitigate crime through targeted resource allocation.[33]

In Kent, the police department adopted predictive policing strategies using the PredPol software, which employs machine learning algorithms to identify potential crime hotspots. The department reported a 20% decrease in burglaries and a 13% reduction in violent crimes over a year following the implementation of the program. By focusing patrols on identified areas, officers could deter potential offenders and respond to incidents more swiftly.[34]

Predictive policing tools helps the law enforcement agencies to allocate all resources more effectively and efficiently by identifying all the hot spots of criminal activity. This data-driven approach allows the police departments to prioritize their efforts in the areas which are predicted for getting experience higher in crime rates. As a result of this all the resources can be concentrated in high-risk neighbourhoods, potentially deterring crime through increased police presence. Traditional patrol methods often relied on officer discretion and experience. However, with the predictive policing the patrol strategies have evolved to incorporate all the algorithm-generated insights. Officers can also be assigned to the specific locations at

[32] Supra note 20
[33] Ibrahim Raji," Predictive Policing: The Role of AI in Crime Prevention", 13 International Journal of Computer Applications Technology and Research 68
[34] Supra note 22

particular times basically based on the predictive analytics which is allowing for a more strategic deployment of personnel. This shift is helping in to create a proactive rather than reactive approach to the basics of crime prevention.

2. AI in Surveillance and Monitoring

Modern surveillance systems are increasingly reliant on the advanced AI technologies which can enhance all their functions and effectiveness. These technologies basically enable more sophisticated monitoring and analysis which is leading to improved security outcomes. The Machine learning algorithms can adapt and improve over time as we all can see daily with the growing and developing AI chats making surveillance systems smarter. The Automated alerts can also notify the security personnel of potential threats so that the preparation becomes easier which helps to reduce the response times. Data analytics tools provide all the insights into patterns and trends which helps in aiding in strategic planning. Integration with IoT (internet of things) devices to allows for a more comprehensive surveillance networking. The adoption of AI technologies in surveillance systems, including AI video management systems and AI home security cameras is transforming how the organizations approach security and making it more proactive rather than reactive. Rapid Innovation assists clients in harnessing all these technologies to achieve greater ROI (return of investments) through the enhanced operational efficiency and reduced risks.[35]

The study found that at least 75 out of 176 countries around the world are actively using artificial intelligence technologies for surveillance purposes[36]. This includes the use of smart city/safe city platforms, facial recognition systems and smart policing. China is considered a major driver of AI surveillance globally, with Chinese companies supplying AI surveillance technology to 63 countries. In particular, Huawei is responsible for providing artificial intelligence-based surveillance technology to at least 50 countries, and non-Chinese companies such as IBM, Palantir, and Cisco are also active in this field.[37]

The AI in surveillance has revolutionized the public safety by enabling its smarter and faster

[35] Jesse Anglen," Role of AI in Surveillance Systems" rapid innovation, available at https://www.rapidinnovation.io/post/role-of-ai-in-surveillance-systems
[36] Steven Feldstein, "Introducing the AI Global Surveillance (AIGS) Index", The Global Expansion of AI Surveillance, pp. 5–7, (Carnegie Endowment for International Peace,2019)
[37] Steven Feldstein, "Introducing the AI Global Surveillance (AIGS) Index", The Global Expansion of AI Surveillance, pp. 13-15, (Carnegie Endowment for International Peace,2019)

threat detections. AI-powered cameras are equipped with the function of facial recognitions and the behavioural analysis which can monitor all the public spaces for identifying the suspicious activities of individuals in real time. AI systems are also been deployed in airports to detect all the unattended luggages which can be a security threat to us, Airports like Changi in Singapore and Incheon in South Korea are examples of facilities that have successfully implemented advanced security systems, ensuring a seamless and secure travel experience for millions of passengers each year[38] They also analyse the crowd behaviour to spot all the abnormal like sudden movements overcrowding or altercations and ensuring rapid response from law enforcement. AI-powered surveillance helps us manage all the urban traffic by analyzing road the conditions monitoring all the vehicle flow and detecting all violations like speeding or jaywalking (people walking on roads). Smart cameras give alerts to authorities in real-time to improve safety and reduce the congestion. In 2023, Dubai introduced AI-based traffic surveillance systems capable of predicting accident-prone areas using historical data and real-time monitoring[39].

AI has numerous applications in the realm of forensic science. Because of artificial intelligence (AI), it is now possible to accurately identify handwriting, recognize faces and voices, estimate age from teeth, and more. Today, a 3D image and the superimposition technique are used to identify an unknown individual from a skull bone. In this age of artificial intelligence, trace evidence—such as blood and bodily fluid stains, lip prints, gunshot remnants, weapon marks, etc.—can be examined and compared more quickly and precisely than forensic specialists[40].

Identification and comparison of specific types of patterns of suspected data are crucial elements of forensic science.

In December 2018, the UP Director-General of Police Om Prakash Singh launched an AIpowered mobile application named ‘Trinetra 2.0’. Trinetra 2.0 has a record of 5 lakh criminals which contains a picture, address, and criminal history of each criminal. This

[38] SUPRA 24

[39] Zainab Husain,” UAE: Eight traffic offences detected by Dubai Police’s advanced AI radar system”, Gulf News , March 10, 2025, available at https://gulfnews.com/living-in-uae/transport/uae-eight-trafficoffences-detected-by-dubai-polices-advanced-ai-radar-system-1.500056465

[40] Dr. O. Gambhir Singh,” Artificial Intelligence in Forensics & Criminal Investigation in Indian Perspective”, 7 International Journal of Innovative Science and Research Technology,2022

information has been collected through the inputs from district police, prison department, and Government Railway Police.[41]

IMPACT OF AI ON PRIVACY: CHALLENGES

The rise of artificial intelligence (AI) is one of the most dynamic developments of the 21st century. From self-driving cars to voice assistants to diagnostics and medical tests. AI promises to transform nearly every aspect of our lives in better and efficient ways. But like any powerful technology, AI has its dark side, a side which is unknown to many. Growing concerns about AI are not just about its impact on business or its ethical implications but it is also about the cybersecurity threats and privacy risks which it adds to our everyday life. In this we will delve into these concerns and explore how AI is a tool to protect and attack our digital infrastructure and how we can protect ourselves in a world of increasing machine intelligence.

AI systems rely on large amounts of operational data , a data which is often personal, sensitive, and often unconsciously acquired. As AI systems become more sophisticated, they can analyse this data at good scale, creating detailed insights about individuals and groups, often without their consent and this is totally unethical.

One of the biggest concerns is the use of AI for surveillance. Facial recognition technology, powered by AI, is becoming mainstream, with governments, companies, and individuals using it to track and monitor people. This raises an important question about the right to privacy. While these technologies can be used for security purposes, such as identifying criminals or preventing terrorism, they also open the door to widespread surveillance by governments or companies.

Clearview AI's facial recognition technology collects all the publicly available images from the internet to create a vast database, raising serious privacy concerns and fears of mass surveillance in many ways. The use of individuals' photos without his or her knowledge or consent has sparked a widespread criticism in our world. Law enforcement agencies have adopted the technology for identification, prompting debates over how to balance the public safety with individual privacy rights. As a result to this, Clearview AI has faced legal actions

[41] Editorial, "Now, UP police to use criminal tracker 'Trinetra' app", Hindustan Times, Dec 28, 2018

and regulatory pressure, emphasizing the growing need for clear guidelines on the ethical use of facial recognition.[42]

AI systems are also used to collect the vast amounts of personal data from social media platforms like Facebook Instagram etc. , online interactions, and other digital footprints. This data is then used to predict behaviour, target advertisements, and influence decisions by showing you there profitable products again and again. The problem arises when this data is not adequately protected or when it's used for purposes that individuals are not aware of or have not consented to. In California, for instance, a former surgical patient reportedly discovered that photos related to her medical treatment had been used in an AI training dataset[43] It can be difficult to assign blame and accountability for judgments made by AI systems, particularly when these systems are in operation, independently. That's why one of the important challenge with AI is accountability.

CHAPTER – 4

AI REGULATIONS ACROSS BORDERS

AI is quickly spreading across many industries like healthcare, finance and transportation this has started a global discussion about how it should be regulated in good manner. Different countries have different rules some of them focus on encouraging innovation, while others are more concerned about the privacy and ethics all depending upon priorities of citizens and nation. This lack of a shared global approach makes it very difficult to manage out AI across borders. Since AI works across countries, there's a very strong need for rules and regulations to handle out all the issues like safety, fairness and responsibility. This chapter looks at how different countries are handling the AI regulation and why working together is an important aspect for safe and fair development of the world without any risk factor.

United States AI Regulations

The U.S. does not have AI law but it regulates AI through agencies like:

[42] Katherine Tangalakis-Lippert," Clearview AI scraped 30 billion images from Facebook and other social media sites and gave them to cops: it puts everyone into a 'perpetual police line-up'", Business Insider, 2023
[43] Benj Edward, "Artist finds private medical record photos in popular AI training data set." Ars Technica, 2022

1. Federal Trade Commission (FTC):

The Federal Trade Commission (FTC) is an independent U.S. government agency which is tasked with protecting of consumers and enforcing the antitrust laws. It basically investigates all the unfair business practices which includes deceptive advertising and promotes the competition across various industries. The FTC works to ensure the AI transparency by requiring clear and understandable disclosures about how the algorithms operate and to prevent all the biased decision making by holding companies whole accountable for discriminatory practices. Their oversight mostly promotes fairness accountability and trust in emerging the AI technologies globally[44].

2. National Institute of Standards and Technology (NIST):

The National Institute of Standards and Technology (NIST) is an U.S. federal agency which develops the critical measurement standards, guidelines and technology to promote innovation, quality and efficiency across all the industries. NIST provides an AI risk management framework for guiding organizations to identify the assess and mitigate all the risks which are associated with the artificial intelligence ensuring the responsible development, deployment and use of emerging technologies effectively worldwide.[45]

3. White House AI Bill of Rights

This is a Bill made for the Protection of citizens from harmful AI practices, it provides basic 5 basic protects to Americans:

1. Individuals should be shielded from systems that are unsafe or inefficient.

2. Systems should be used and made fairly, and algorithms shouldn't discriminate against individuals.

[44] Mark D Gray, Chief Artificial Intelligence Officer, Compliance Plan For Omb Memoranda M-24-10: On Advancing Governance, Innovation, And Risk Management For Agency Use Of Artificial Intelligence, , Federal Trade Commission, September 2024

[45] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1. U.S. Department of Commerce, 2024, available at https://doi.org/10.6028/NIST.AI.600-1.

3. Individuals should have control over how their data is used and remain protected from abusive data practices by built-in safeguards.

4. Individual should be aware of when an automated system is being used and comprehend how and why it affects results that affect a person.

5. Individual should have access to someone who can promptly assess and address issues they face, as well as the option to opt out when necessary.

White House AI Bill of Rights protects all the citizens from the harmful AI practices by establishing some clear guidelines for safe, ethical technology use.[46]

Individual states like California, have proposed changes and addition in privacy laws called as the California Consumer Privacy Act (CCPA) and added AI in the definitions etc, also it outline the rules and guidelines for businesses to follow when collecting, using, and sharing consumer personal information, including the use of automated decision-making technology[47].

China's AI Laws

China's AI regulations basically focus on the national security, data control, and AI ethics. China is the first country to implement detailed, binding regulations on some of the most common applications of AI in 2023.[48]

Interim Measures for the Management of Generative AI Services – in this it is, required by the AI developers to follow all the government-approved ethical standards before any data feeding and even creating of an AI. Article 2 of measures provide, Services that offer generated text, photos, audio, video, and other content to the general public inside China are covered by its regulatory reach. Research and development (R&D), enterprise, and industrial applications that do not directly offer services to the general public are not covered by the Measures. The rule addresses a number of issues related to the use of generative AI, such as intellectual

[46] Dr. Alondra Nelson," Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age", The White House ,2022
[47] California Privacy Protection Agency ,"California Consumer Privacy Act Regulations", 04.04.2024 ,available at https://cppa.ca.gov/meetings/materials/20250404_item6_draft_text.pdf
[48] Matt Sheehan," Tracing the Roots of China's AI Regulations", Carnegie Endowment for International Peace, 2024

property violations, data security, content security, and personal data protection. In order to reduce these risks, it also establishes a multi-tiered framework of duties for generative AI service providers.[49]

Japan AI Guidelines

Similarly, In 2023 to coincide with the G7 Summit, Japan published the Hiroshima International Guiding Principles for Organizations Developing Advanced AI Systems, which aim to establish and promote guidelines worldwide for safe, secure, and trustworthy AI. The government of Japan stepped up its attempts to enact laws allowing AI in 2024. The first draft of the "Basic Law for the Promotion of Responsible AI" (AI Act) was made public by the government in February. The AI Guidelines for Business Ver 1.0, released in April 2024 by the Ministry of Economy, Trade, and Industry, was designed to provide advice to all organizations involved in creating, supplying, and utilizing AI.[50]

These guidelines bring together the earlier ideas and advice from the experts to help the businesses to use AI responsibly, especially new technologies like the generative AI. They focus basically on ten important principles which are: keeping AI centred on human values, making it safe, fair, private, secure, transparent, and accountable, promoting AI education, ensuring fair competition and encouraging the innovation. These guidelines also give specific advices for different groups involved in AI like the developers, service providers and the business users.[51] Despite these measures, governments face challenges such as the lack of global AI standards, persistent issues with AI bias and fairness, rapid technological advancements are outpacing regulation, and its getting way to difficult in enforcing compliance, all of which the regulators must address to create an effective AI policy.

[49] Mimi Zou and Lu Zhang," Navigating China's regulatory approach to generative artificial International Peace, 2024 intelligence and large language models", Cambridge University Press, 06 January 2025, available at https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/navigating-chinas-regulatory-approach-to-generative-artificial-intelligence-andlarge-language-models/969B2055997BF42DE693B7A1A1B4E8BA

[50] Nick Sherman, "AI Regulations around the World – 2025", mind foundry, 2024

[51] AI Guidelines for Business Ver 1.0", Ministry of Internal Affairs and Communications Ministry of Economy, Trade and Industry,2024

Europe

The European Union Artificial Intelligence Act[52] establishes comprehensive regulations for AI systems across the Europe, with the first section of banning certain AI systems—coming into effect on 1 August 2024. Key features include harmonised rules for all member states, prohibition of high-risk AI applications, AI governance and market surveillance framework, specific requirements for high-risk systems, and transparency obligations for certain AI technologies. The EU AI Act has divided AI systems into three danger categories: low risk, high risk, and unacceptable risk. Systems with unacceptable risk are considered dangerous and are simply prohibited. These include systems that engage in behavioral manipulation, biometric identification, facial recognition, and social scoring. Evaluations would only need to be performed on powerful generative models like GPT-4. The EU's rights-driven strategy aims to promote innovation while striking a balance between safety and security.[53]

Australia

Australia has implemented several laws to support the responsible AI governance. At the heart of its regulatory approach is the National Artificial Intelligence Ethics Framework[54], which basically outlines the core of the ethical principles for developing and using the AI technologies. The principles are: (a) generation of net benefits; (b) doing no harm; (c) regulatory and legal compliance; (d) privacy protection; (e) fairness; (f) transparency and explainability; (g) contestability; and (h) accountability[55]. This framework aims to ensure that AI is used in a responsible and trustworthy manner which is. helping to build public trust. Australia strives to create an environment which encourages AI innovation with safeguarding all the consumer rights and upholding the ethical standards.

CHAPTER – 5

LEGAL FRAMEWORK IN INDIA

AI applications in our India often face some significant privacy challenges. These AI

[52] European Union regulation on artificial intelligence, 2024
[53] "AI Regulations: Global Trends, Challenges, and Approaches." BowerGroupAsia, available at https://bowergroupasia.com/ai-regulations-global-trends-challenges-and-approaches/
[54] Dawson D and Schleiger E," Artificial Intelligence: Australia's Ethics Framework" , CSIRO, 2019
[55] "Australia's AI Ethics Principles", Australian Government :Department of Industry, Science and Resources

applications can accidentally expose personal information such as location data, social media profiles and contact details, which malicious actors may misuse for stalking, harassment, or threats. Additionally, if the AI systems leak or mishandle the sensitive data, with embarrassing or private content affecting an individual's personal and the professional life. it can cause serious reputational damage as we had case from a very famous personality of India Arjit Singh. the Bombay High Court ruled in favor of singer Arijit Singh in a case against Codible Ventures LLP. The court addressed the unauthorized use of Singh's voice through AI technology, where his voice was replicated without consent for commercial purposes. This landmark decision highlighted the legal challenges surrounding voice cloning and the need to protect artists' rights in the era of AI.[56]Moreover, the misuse of sensitive information like health records, religious beliefs, or political affiliations can result in discrimination, unfair treatment, and social exclusion. These issues highlight the urgent need for some stronger privacy protections and robust regulations around the use of AI in our India.[57]

AI systems in India often need huge amounts of personal information, but the people usually don't know that exactly how their data is collected, shared or used, which leads to an unauthorized data gathering and misuse of the private details. The Digital Personal Data Protection Act of 2023 was meant to regulate all of this, but it let the government bodies and all the research projects process personal data without full or informed consent or strong safeguards through all the broad exemptions. It allows government bodies and research projects to process personal data without full or informed consent and without strong safeguards. Key sections like Section 17 [58] permit data processing for reasons such as national security, research, and public interest, often without user knowledge. These exemptions risk unauthorized data collection, misuse, and lack of accountability.

At the same time, facial-recognition programs like the National Automated Facial Recognition System and airport "Digi Yatra" selfies scans and stores people's faces without any clear informed permission, risking false matches and constant surveillance[59]. Because transparency is very low, many users aren't aware that their data can be repurposed or shared, increasing the fear of misuse and loss of privacy. Another big problem is that there aren't any clear rules

[56] Arijit Singh v. Codible Ventures LLP and Others, 2024
[57] Sh. Sant Vijay Singh, "Data Protection and Data Privacy ",9 International Centre for Information Systems and Audit 62, 2024
[58] The Digital Personal Data Protection Act , 2023 , s.17
[59] Jagriti Chandra," Privacy concerns over Digi Yatra initiative", The Hindu , 2024

about how the AI companies in India store or move the data of people. Many companies use cloud services from other countries, so the personal data can be sent outside of India, where Indian laws can't fully protect it. This makes people worry about how safe their information really is. Also, AI is being used in the banks and hospitals to handle some sensitive things like money details or health records, but it's not always clear how safely this data is kept and where. Without strict rules, this information could be leaked, sold or can be used in ways people didn't agree to ever in life. On top of that, AI is now being used to make an important decision, like who gets a loan or gets selected for a job. But people often don't know why they were rejected or if the AI has used unfair or incorrect data. This lack of clarity can lead to unfair treatment, and it also shows why stronger privacy rules are needed for AI in our India.

In this digital era, India takes a step towards the technological innovation and economic growth. its legal framework is basically tasked with the delicate balance of artificial intelligence and development while safeguarding the fundamental privacy rights which is embedded in article 21 of Indian constitution[60].

CURRENT SITUATION OF AI REGULATIONS IN INDIA

India's approach to regulating AI is still very new, with laws that are spread out and no specific framework is made only for AI. Even though AI is seen as a game-changing technology to the whole world but the rules governing it mainly depend on older laws which weren't created to handle the special challenges which come out with AI systems.

1. **The Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act 2023 is a law which was passed in India to protect the people's digital personal data. This includes any information which can be used to identify a person, for an example their name, phone number, email, Aadhaar number, or locations where they live. The Act applies to personal data which is collected, stored or processed in the digital form, whether it happens inside India or outside of our country if it involves the data of an Indian citizen or citizens.

This law is very much important because it basically ensures that all the people are aware of how their personal data is being used and about that the companies ask for clear permission

[60] The Constitution of India, art.21

before using it. Also, the data is being kept safe and private and that individuals can also file complaints or ask for corrections if something goes wrong with them or the data.

Although the Act doesn't specifically mention about Artificial Intelligence (AI), it still applies to situations where the AI systems process all the personal data. For an example, if an AI tool uses someone's personal data to make decisions such as approving loans, reviewing resumes, or personalizing content the organisation behind the AI must follow all the rules of the DPDP Act 2023.

The Digital Personal Data Protection Act, 2023, introduces several key definitions, including "automated" and "artificial juristic person". The definition of "automated" is any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data[61]. It encompasses AI systems that can operate automatically in response to instructions, while "artificial juristic person[62]" refers to AI systems that can acquire rights and incur liabilities. it allows AI systems to be considered "legal persons" for the purposes of the law, ensuring they are held accountable for their actions[63]. Even though the DPDP Act 2023 doesn't directly mention AI in it but it plays an important role in regulating how the AI systems handle personal data in India. Any organisation using AI which processes the people's data must follow the Act by getting consent plus protecting data and using it only for the right purposes and respecting all the rights of users.

2. **Information Technology Act, 2000**

The Information Technology Act, 2000 is India's main law for the digital activities. It covers mostly all the issues like cybercrimes, data breaches and the responsibilities of online service providers at times. However, this law does not have any specific rules for regulating AI systems, such as ensuring algorithmic accountability, reducing bias in most of the sectors of decision's and reasonings, or determining who is responsible for an autonomous system. A vital role of this act is that it gives legal validity to contracts made through electronic means. this defines the responsibilities of online platforms (like social media companies) in handling the user content and protecting the users data.

[61] Digital Personal Data Protection Act, 2023, S. 2(b)
[62] Digital Personal Data Protection Act, 2023, S. 2(s)(vii)
[63] Prabuddha Ganguli," Recognising generative and autonomous AI as a 'juridical person'", 6 Journal of Data Protection & Privacy 406-407(2024)

Section 43A[64] of the IT Act provides compensation in the event of a breach of data privacy caused by careless treatment of sensitive personal information. This provision is especially important in the context of AI systems that handle user data.

Judiciary's Role

1. *Justice K.S. Puttaswamy v. Union of India[65]*

- This case dealt with the issue of the right to privacy under Article 21 of the Indian Constitution. The judgment emphasized that privacy is a fundamental right and laid down principles for data protection, which is crucial for the regulation of AI systems, especially those that rely on vast amounts of personal data.

- In 2012, Judge K.S. Puttaswamy filed a petition before a nine-judge Supreme Court against the Union of India, arguing that Aadhaar was unconstitutional due to its violation of the right to privacy.

- It was decided that informational privacy is a component of the right to privacy and that the claim of privacy protection can be made against both state and non-state actors because, in the age of technological advancement, threats can come from both non-state and state actors. The right of an individual to control his or her data and online presence may be violated if such information is used without authorization.

- This ruling is particularly relevant for AI because many AI applications require large datasets, including personal information. The court's decision on privacy and data protection will inform future regulatory frameworks for AI systems in India.

While these efforts are useful but they are not consistent across all the areas and do not cover all the challenges which cut across the different sectors.

CHAPTER – 6

CONCLUSION AND SUGGESTIONS

Artificial intelligence in India is at a turning point. On the one hand, it promises some big

[64] 43A. Compensation for failure to protect data.
[65] 2017 SC 801

improvements in health care, education, public services, and many more. On the other, it raises some real worries about our privacy. AI's power comes from its ability to collect huge amounts of personal information, spot patterns and make decisions automatically. In India, where more people than ever are using their smartphones and online services, this means both great advantages and serious risks at a single point in time. AI can help doctors find diseases sooner, tailor lessons to each student, or speed up government work. Still, it can also gather, store, share, and use our most private details, like fingerprints, medical records, and banking histories, sometimes without clear permission. Finding the right balance between using AI's benefits and protecting our privacy is the key challenge here. Each phone tap, voice command, or photo adds to a digital trail. AI systems can link these trails to guess where we go, what we like, or how much credit we deserve sometimes in helpful ways, sometimes not helpful at all. But most people don't know how far their data travels, who can see it, or how long it is kept out. In a country where not everyone understands any of these issues, this uncertainty creates fear: fear of being watched, profiled unfairly, or even having one's identity stolen.

India's main answer to this so far is the Digital Personal Data Protection Act of 2023. It sets rules for how companies and government agencies must collect, process, store, and share personal data. It requires informed consent, limits on how much data can be kept, and fast breach notifications. But there are big carves out, especially for government work, national security, and some research projects that weaken these protections. Unless these loopholes are closed, powerful AI tools in policing or welfare could keep using our data without real checks and balances. Whether the law truly protects privacy depends on how strictly those exceptions are defined and enforced in our nation. A vivid example of this tension is India's National Automated Facial Recognition System and related projects like "Digi Yatra" at airports. By linking thousands of CCTV cameras and boarding cabins to a central database of faceprints, these systems aim to boost security, speed up lines, and stop fraud. But they also turn public spaces into zones of constant, hidden surveillance. Errors in face-matching can wrongly flag innocent people, and continuous tracking threatens our freedom to move, speak, or protest without fear. Even after the Supreme Court in 2017 declared privacy a fundamental right, India still lacks clear rules, outside audits, and easy ways to challenge mistakes in these face recognition systems.

Looking back over the decades shows how hard it has been to keep up. Early AI systems in the 1960s only needed small data inputs. Today's deep-learning models and chatbots feed on

millions of bits of user-generated content and sensor readings. Milestones like ELIZA in 1966, expert systems in the 1970s, big-data breakthroughs in the 2000s, and today's generative transformers have each widened the gap between the speed of innovation and the strength of privacy safeguards. In India, the 2017 Puttaswamy decision and the 2023 data-protection law are steps forward—but slow rule-making and political hesitation have left gaps as technology moves faster.

In law enforcement, predictive policing algorithms, biometric tracking, and data analytics promise to anticipate crime and use resources more efficiently. Yet the same tools can disproportionately focus on marginalized groups, based on biased training data, leading to over-policing and wrongful stops. Everyday surveillance erodes the anonymity that underlies free movement and speech. To use these tools responsibly, India needs clear limits on what data can be collected, independent checks for bias, full disclosure of how algorithms work, and strong legal safeguards against misuse. Independent watchdog bodies with real power to audit and sanction are essential to prevent mission creep.

Looking around the world offers useful ideas. The European Union's AI Act uses a risk-based approach, with strict rules for high-impact systems and heavy penalties for violations. The United States relies more on voluntary standards and sector-specific rules, which can move fast but may miss systemic gaps. China enforces tight government control over data, often at the expense of personal privacy. The UK and Japan use principle-based guidelines and public consultations to shape ethical AI. Australia works closely with industry and researchers on flexible, principle-driven rules. India can combine the EU's clear risk tiers, the UK's public involvement, and Australia's collaborative spirit—while avoiding overly broad exceptions.

At home, bodies like NITI Aayog's "AI for All" and special task forces on ethical AI show India's strong interest. Draft guidelines call for transparent decision-making, human oversight to catch bias, and data localisation to keep control within the country. But without a single, enforceable law, these remain goals more than requirements. Differences across states in digital ID programs, uneven internet access, and gaps in technical expertise make consistent implementation a challenge. India must bring together civil society, academia, and industry so policies reflect diverse views and real-world needs.

Moving ahead, India should quickly finalize and strengthen its data-protection law—closing unnecessary carve-outs and clearly defining terms like "sensitive personal data" and

"profiling." A truly independent data-protection authority must have the power to investigate, audit, and fine offenders. Mandatory third-party audits of high-risk AI systems—with public reports on fairness and accuracy—will build trust. Data-localization rules must balance national security with support for startups. Consent must be simple, specific, and revocable. Public education campaigns should explain data rights, show people how to spot misuse and guide them in seeking redress.

In the end, India's task is to embrace AI's benefits while protecting each person's dignity, independence, and freedoms. Privacy must be built in from the start of any AI project—never an afterthought. By learning from global best practices, involving all stakeholders in ongoing dialogue, and enforcing solid rules with real consequences, India can create a future where technology and civil liberties grow side by side. It will take flexible laws, strong institutions, and active civic engagement—but the reward is huge: an inclusive, innovative India where every citizen can enjoy AI's promise without sacrificing the privacy that supports a true democracy

SUGGESTIONS

1. **Strengthen the Digital Personal Data Protection Act (DPDPA) with AI-Specific**

   Provisions: As we know the current DPDP law covers personal data generally but doesn't spell out how the AI systems which often process massive datasets must handle all the user information. Basically, amending it to require a clear consent protocol for AI training, define lawful exemptions for research and limit all unreviewed automated decisions this will help to ensure individuals that there data isn't misused.

2. **Mandate Privacy-by-Design [66]in AI Development**: All stages of the AI system lifespan, from idea and development to deployment and maintenance, must include Privacy-by-Design (PbD) concepts. This method encourages risk mitigation that is proactive as rather than reactive. Indian AI engineers must be required to carefully recognize, evaluate, and reduce privacy issues at every turn. Boost trust in AI systems, By outlining the legal requirements for responsible AI development, companies may promote innovation and Lower the chance of data breaches, abuse, or discriminatory consequences involving

[66] Dr. Ann Cavoukian, "Privacy by Design: The Seven Foundational Principles", The Sedona Conference Institute, 2010

personal data. Rather than bolting on the privacy safeguards at the end, developers must integrate the data minimization, anonymization techniques and robust the security checks from the very start of an AI project.

3. **Ensure Algorithmic Transparency and Accountability:** AI systems should clearly explain how they use the data to reach any sort of decisions. Users deserve to know when they're interacting with a machine and what data makes its output and who can be held responsible if something goes wrong within or after the process. Transparent models build a very good trust and enable meaningful redresses Establish a national framework for independent audit of AI systems to assess fairness, transparency, bias, and compliance with ethical and legal norms.

4. **Establish Robust Institutional Oversight:** Forming an Inter Ministerial AI Coordination Committee, led by the Ministry of Electronics and Information Technology and the Principal Scientific Adviser, alongside a dedicated Technical Secretariat, will harmonize all the AI rules across every sector. These bodies can horizon-scan the emerging risks, develop common standards and lastly advise on the law and policy updates to keep privacy protections in practice.

5. **Conduct Mandatory Privacy Impact Assessments (PIAs) for AI Projects:** Before rolling out any AI system, organizations should map or we can say plan that exactly how the personal data will flow through the algorithms and flag a potential privacy pitfall. A PIA helps design in necessary safeguards, demonstrates compliance and fosters the trust by showing due diligence to regulators and users.

6. **Promote the Use of Non-Personal Data (NPD) for AI Training:** Whenever it is possible, AI models should be trained on datasets that have been faked or synthetically generated so they contain zero direct personal identifiers. This reduces the chance of reidentification and privacy breaches, while still powering the innovation with rich, high quality of data.

7. **Enhance Public Awareness and Empower Individual Control:** Citizens should be educated in very simple terms about how the AI uses their data and what rights they all have under the DPDP Act. Clear, jargon-free consent forms, straightforward tools for accessing or deleting personal information and a nationwide awareness campaigns will help the people take charge of their digital privacy in the best manner.

BIBLIOGRAPHY

1. K.S. Puttaswamy v. Union of India [2017} 10 SCC 1

2. Kashish Maggo, "Artificial Intelligence: Impact on Right to Privacy", Juris Centre, [12 September 2023] , available at[https://juriscentre.com/2023/09/12/artificial-intelligenceimpact-on-right-to-privacy/]

3. Rohith S B & Sethupriya N, "A Study On Impact Of Artificial Intelligence On Right To Privacy In India", Indian Journal Of Legal Review, 2024

4. Avinash Dadhich & Vasanthika Srinath , "Impact of Artificial Intelligence on Privacy Harms: A Taxonomy of Intrusion & Privacy Risk Assessment Framework"[2024] [published Master of Laws (LL.M.) dissertation, Manipal Law School MAHE, Bengaluru]

5. D. Majumdar and H.K. Chattopadhyay, "Emergence of AI and its Implication Towards Data Privacy: From Indian Legal Perspective" 3 International Journal of Law Management & Humanities 1-20 (2020).

6. Helen Nissenbaum, "Privacy in Context Technology, Policy, and the Integrity of Social Life" (Stanford University Press, Stanford, California, 2009).

7. Daniel J. Solove ,"Understanding Privacy" ,Harward University Press ,2010

8. Daniel J. Solove, "Artificial Intelligence and Privacy", *Florida Law Review* (2025)

9. "AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data" , *The Economic Times,* Apr 25, 2023, *available at: https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concernssurrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms*

10. *"*The Dangers Of Artificial Intelligence To Humanity – A Comprehensive Analysis Of The Threats Posed By AI*", AI for Social Good* ,11th January 2024 *, available at*

https://aiforsocialgood.ca/blog/the-dangers-of-artificial-intelligence-to-humanity-acomprehensive-analysis-of-the-threats-posed-by-ai

11. Fatima Dakalbab, Manar Abu Talib, Omnia Abu Waraga, Ali Bou Nassif, Sohail Abbas, Qassim Nasir, Volume 6, Issue 1, *"Artificial intelligence & crime prediction: A systematic literature review",* Social Sciences & Humanities Open, 8 October 2022.

12. Gregory J. Garmon," The Ultimate Guide to Government Surveillance: Learn How to Protect Your Privacy Today!", *Surveillance Guides,*2023, *available at https://surveillanceguides.com/guide-for-government-surveillance/*

13. Prof Dalvinder Singh Grewal," A Critical Conceptual Analysis of Definitions of Artificial Intelligence as Applicable to Computer Engineering*", IOSR Journal of Computer Engineering e*-ISSN: 2278-0661, Volume 16, Issue 2, 2014

14. Michael Haenlein and Andreas Kaplan, *"*A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence", *California Management Review,* 2019, Vol. 61(4)

15. Stanford University," Artificial Intelligence and Life in 2030: The One Hundred Year Study on Artificial Intelligence(AI100)"12(2016).

16. Stuart Russell and Peter Norvig," Artificial Intelligence A Modern Approach*", Pearson Series In Artificial Intelligence 54,*2022

17. Andreas Kaplan and Michael Haenlein,"Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence", *62 Business Horizons 15* ,2019

18. Patrick Mikalef and Manjul Gupta," Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance,*58 Information and Management* , 2021

19. A. M. Turing, "Computing Machinery And Intelligence", 59 *Mind*, 1950

20. Ellen Glover," What Is AI Winter?" , *Builtin,* 2023

21. Billy Perrigo**,** "The UAE Is on a Mission to Become an AI Power"**,** *Time ,*March 20 ,2024.

22. Manisha Salecha," Story of ELIZA, the first chatbot developed in 1966", *Analytics India Magazine,* October 5, 2016 available on https://analyticsindiamag.com/ai-features/story-eliza-firstchatbot-developed-1966/

23. Stanford. "Shakey the Robot", available at https://ai.stanford.edu/~nilsson/OnlinePubsNils/shakey-the-robot.pdf.

24. IBM. "Deep Blue." *IBM History*, available at www.ibm.com/history/deep-blue.

25. IBM, "Watson on Jeopardy*!*" *IBM History*, available at https://www.ibm.com/history/watson-jeopardy

26. Macro Del Pra, "Generative Adversarial Networks." *Medium*, 17 Oct. 2017, available at https://medium.com/@marcodelpra/generative-adversarial-networks-dba10e1b4424

27. DeepMind. "AlphaGo." *Google DeepMind*, available at https://deepmind.google.com/research/breakthroughs/alphago/.

28. Rahib Imamguluyev, "The Rise of GPT-3: Implications for Natural Language Processing and Beyond",4 *International Journal of Research Publication and Reviews* (2023)

29. Md Asraful Haque, "A Brief Analysis of ChatGPT – A Revolutionary Tool Designed by OpenAI"*, EAI Endorsed Transactions on AI and Robotics* (2023)

30. Walter L. Perry, Brian McInnis, Carter C. Price, Susan Smith, John S. Hollywood.et.al,"

Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations", *Rand* 1,2(2013)

31. Ibrahim Raji," Predictive Policing: The Role of AI in Crime Prevention", 13 *International Journal of Computer Applications Technology and Research 68*

32. Steven Feldstein, "Introducing the AI Global Surveillance (AIGS) Index", *The Global Expansion of AI Surveillance,* pp. 13-15, (Carnegie Endowment for International Peace,2019)

33. Zainab Husain," UAE: Eight traffic offences detected by Dubai Police's advanced AI radar system", *Gulf News ,* March 10, 2025, available at https://gulfnews.com/living-inuae/transport/uae-eight-traffic-offences-detected-by-dubai-polices-advanced-ai-radarsystem-1.500056465

34. Dr. O. Gambhir Singh," Artificial Intelligence in Forensics & Criminal Investigation in Indian Perspective", 7 *International Journal of Innovative Science and Research Technology*, 2022

35. Editorial, "Now, UP police to use criminal tracker 'Trinetra' app", *Hindustan Times,* Dec 28, 2018

36. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1. U.S. Department of Commerce, 2024, available at https://doi.org/10.6028/NIST.AI.600-1

37. California Consumer Privacy bill,2024

38. Matt Sheehan," Tracing the Roots of China's AI Regulations", Carnegie Endowment for International Peace,2024

39. Mimi Zou and Lu Zhang," Navigating China's regulatory approach to generative artificial intelligence and large language models", Cambridge University Press, 06 January 2025, available at https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-andgovernance/article/navigating-chinas-regulatory-approach-to-generative-artificialintelligence-and-large-language-models/969B2055997BF42DE693B7A1A1B4E8BA

40. Ed Glasgow and Dr. Nathalie Moreno, "The UK'S AI opportunities action plan – innovation catalyst or regulatory gamble?", kennedys law 2025

41. Nick Sherman, "AI Regulations around the World – 2025", mind foundry, 2024

42. European Union regulation on artificial intelligence, 2024

43. "AI Regulations: Global Trends, Challenges, and Approaches." BowerGroupAsia,

available at https://bowergroupasia.com/ai-regulations-global-trends-challenges-andapproaches/

44. "Australia's AI Ethics Principles", Australian Government :Department of Industry, Science and Resources

45. The Constitution of India, art.21

46. NITI Aayog," National Strategy for Artificial Intelligence" (2018).

47. Digital Personal Data Protection Act, 2023, S. 2(b)

48. Digital Personal Data Protection Act, 2023, S. 2(s)(vii)

49. Prabuddha Ganguli," Recognising generative and autonomous AI as a 'juridical person'", 6 Journal of Data Protection & Privacy 406-407(2024)

50. 43A. Compensation for failure to protect data.

51. Saloni Shukla," RBI announces 'FREE-AI' committee to develop AI framework", The Economic Times , Dec 26, 2024, available at https://economictimes.indiatimes.com/news/economy/policy/rbi-announces-free-aicommittee-to-develop-ai-framework/articleshow/116684195.cms

52. Indian Council of Medical Research," The Ethical Guidelines for Application of AI in Biomedical Research and Health care", (2023)

53. Dr. Ann Cavoukian, "Privacy by Design: The Seven Foundational Principles", *The Sedona Conference Institute ,*2010