The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

AI AND PRIVACY LAWS: BALANCING INNOVATION AND DATA PROTECTION

~Yash Gupta

I. Abstract:

In the era of information technology, artificial intelligence (AI)[1] has come to be seen as a revolutionary force reshaping many facets of human existence. As its power increases, worries about its effect on human rights and privacy[2] have grown. This thesis paper examines relationship between AI and privacy legislation, attempting to achieve a fine balance between technology progress and protection of data. The research carries out a rigorous review of the literature to comprehend the historical evolution of AI, its ethical dimension[3], and the legal frameworks[4] that regulate its deployment. Based on real-world case studies, it examines cases wherein AI has helped advance and undermine human rights along with safeguarding their data. The paper explores the imperative of explainable and transparent AI, with emphasis on ethically motivated development and responsible deployment. Through an in-depth analysis of global and local regulatory actions, it discusses the legal environment with regard to AI and privacy rights. The story discusses strong suggestions on how actors can come together to ensure a human centered AI future that includes both innovation and data protection.

Keywords –

1 Artificial intelligence,2 Privacy,3 Ethical implications,4 Legal framework.

II. INTRODUCTION:

The term artificial intelligence was the domain of science fiction novels and Hollywood movies. But with the fast pace of technology in the modern digital world, a new era dawned when AI became a natural aspect of day-to-day life. From recommending personalized content

on streaming services to driverless cars plying the roads, AI has penetrated various sectors of society with a promise to revolutionize it. However, in the midst of the beauty of technological progress lies a shadowy cloud over the future consequences of AI on human privacy legislation and data protection.

The aim of this thesis paper is to discover the complex relationship between AI and Privacy legislations and highlight how we can harmonize innovation with data protection in the face of unprecedented technological transformation. As we make this intellectual journey, it is important to realize the historical background of AI's development:

The origins of Artificial intelligence date back to the first half of the 20th century, when visionaries like Alan Turing established the groundwork for the computational devices to carry out tasks that previously seemed exclusive to human thought. The past decades have been marked by a proliferation in AI research and development with the emergence of big data, cloud computing, and high-capacity computational capabilities.

The arrival of AI has unveiled gigantic scope for upholding and advancing privacy legislation. On the one-hand, AI-based applications are improving education and medical care access in underserved areas, ensuring inclusiveness and equality. Additionally, predictive aspects of AI have the power to transform criminal justice systems, saving people from wrongful convictions and guaranteeing impartial trials.

But we cannot ignore AI's darker aspect. Algorithmic discrimination and biased practices in AI systems are dangerous for privacy regulations. Furthermore, the constant drive for data-driven intelligence has created deep concerns regarding privacy and data protection. As AI algorithms collect enormous amounts of individual data, the risk of surveillance and exploitation has grown.

Throughout this journey, the position of transparent and explainable AI comes forward as a driving force against any possible violation of privacy laws. By requiring transparency and accountability in AI decision-making processes, we can ensure that the black boxes of AI systems remain free from violating the privacy laws.

This essay will explore ethical issues in the development and application of AI. It will examine current legal and regulatory policies of international and national authorities with the objective of determining gaps and potential areas for meeting the impact of AI on privacy legislation and data protection.

By examining real world case studies, we will dissect the positive and negative consequences of AI implementation, revealing valuable lessons and potential strategies for improvement. This examination will underscore the importance of integrating ethical principles into AI design and deployment, advocating for responsible AI practices.

In subsequent chapters, this thesis will explore through impact of AI on law, AI and data privacy issues, Cyber bullying, Data protection Acts, and a Bar graph showing the rise or fall in cybercrimes in last 5 years.

By thorough analysis and thorough research, this story attempts to inspire informed conversations and help inform policies that promote the ethical and responsible development and deployment of AI.

III. LITERATURE REVIEW:

The history of artificial intelligence provides an important context for what it has done to the privacy laws of today. The initial visionaries such as Alan Turing and John McCarthy established the foundation for AI research, and their efforts have culminated in the development of sophisticated AI systems which have surpassed the capabilities of human beings in some areas.

And also, there were a lot of other scientists who had also conducted research on such a sort of thing as Allen Newell and Herbert Simon, who built the General Problem Solver (GPS), which is one of the first AI programs designed to simulate human problem-solving abilities. It formed the basis of the creation of cognitive architectures in AI.

Stuart Russell has been extensively involved in aligning AI systems with human values to the extent of ensuring that AI systems behave in a positive manner towards humanity.

Giovanni Sartor is a legal informatics expert and technology-privacy law relationship expert.

Researchers have widely discussed the ethical aspects of AI, and there has been a call for transparent and accountable algorithms. The publications of Wachter and Mittelstadt pointed out the algorithmic accountability concerns and emphasize that "individuals are granted little control and oversight over how their personal data is used to draw inferences about them" to safeguard privacy law and data protection.

Ethical and legal principles that underpin AI development and utilization have become pivotal topics for research. The European Union's General Data Protection Regulation (GDPR) has been a pioneering legislation on data protection and privacy, with its foundational principles of transparency, fairness, and purpose limitation as a beacon for AI developers to guard against violation of privacy laws.

IV. IMPACT OF AI ON LAW :

Artificial intelligence has revolutionized every professional field including legal profession. Computer program replacing paper work and data management. In the world, legal business experiencing speedy growth and technological innovation. Nothing is left to be replaced by technology except few services which depends upon the experience and judgment. As per the company called 'Deloitte' "More than 100,000 jobs in the legal industry have a strong likelihood of being automated in the next two decades".

Advantages of Artificial intelligence in legal profession industry:

Artificial intelligence is making its entry in the legal field as there are numerous software available through which the lawyers' monotonous and tedious work can be replaced. Artificial intelligence assists the lawyers in repetitive and routine tasks which certainly saves them time, but also assist the lawyers in prioritizing significant areas like Legal research, Due diligence, Legal analysis, Contract preparation etc.

Legal problems with artificial intelligence:

Artificial intelligence are also facing different legal problems throughout the world. Artificial intelligence software employs big data to produce loads of information. These big data laws are changing across the globe. USA has also encountered different legal problems between government and technology companies. These legal problems are most likely to increase with software development and time passage.

Amazon Inc. has been subjected to search warrants for furnishing information in a case of murder involving Artificial intelligence enabled Echo device. There are different related laws to Artificial intelligence that can be depended upon the data privacy legislation.

V. AI AND DATA PRIVACY ISSUES:

With the ongoing development of AI technologies and their increased use, privacy and data protection issues have become top priority. AI technologies tend to use massive amounts of

data, and the question arises how personal data is gathered, processed, and stored. Let us discuss some of the major challenges related to AI and Privacy, highlighting potential weaknesses and challenges that organizations can expect to face in protecting individual's right to privacy.

1.Data Privacy Breaches: AI systems usually utilize very large amounts of data for training purposes and making decisions. Such data may, however, contain sensitive personal information like health records, financial transactions, and biometric data. Inappropriate handling or unapproved access of such data can lead to privacy breaches as well as encroachment upon individual's privacy rights.

2.Algorithmic Bias and Discrimination: AI systems can unintentionally perpetuate discrimination and bias, which results in discriminatory or unjust outcomes, especially where it involves sensitive domains like employment, lending, and law enforcement.

3.Surveillence and Tracking: AI-enabled surveillance technologies like facial recognition and location tracking raise spectres of mass surveillance and violation of privacy rights of individuals.

4.Lack of Transparency: Most AI systems are black boxes, and it is difficult to comprehend how decisions are made or to hold them responsible for their actions.

5.Data Security Vulnerabilities: AI systems are vulnerable to security vulnerabilities and attacks, such as data breaches, adversarial attacks, and model poisoning.

VI. LEGAL FRAMEWORK IN INDIA FOR CYBER OFFENCES :

If we compare India with other European nations and American nations in terms of data protection and cybercrimes or cyber frauds, we may conclude that India is weaker in terms of technological laws and with a high rate of cybercrimes.

Cybercrime is a criminal act that contains computers, internet or any kind of network devices. Primarily cybercrime is done by cybercriminals or hackers who aim to earn money. These crimes entail the utilization of technology to perform online fraudulence, identity theft, computer virus and other several forms of deception.

The cybercriminals abuse the computer networks to achieve unauthorized access and pilfer sensitive data that leads to financial loss and damage the reputation of any person, organizations as well as governments. As our nation became more and more connected with internet and

digital technologies, cyber criminals got new opportunities to monitor any sensitive data that assist them to achieve power to dominate.

There are numerous categories of cybercrime like email and internet fraud, identity fraud, Theft of financial or card payments, Cyberextortion, Cyber bullying, Infringing copyright etc.

For empowering India's Legal Framework for combating Cybercrime, the following legal reforms are required:-

• To Update the Information Technology Act – Increase the ambit of law to incorporate burgeoning cybercrime threats and technologies as well as provide more precise definitions and jurisdictions for various cybercrime cases.

• Criminal Procedure Code- Greatly need for the criminal procedure code to be amended to carry out the process of gathering, maintaining, and producing digital evidence in courts and authorize the police to carry out real-time electronic surveillance and monitoring with precautions.

• Need to enact more cybercrime legislation- To create a full-fledged cybercrime act, which defines cybercrime act, which defines cybercrime offences, digital evidence procedure, jurisdiction rule, penalties and imprisonment.

• Strengthening punitive measures- To provide for more stringent prison terms and fines for various cybercrime offences and also assets and proceeds acquired by cybercrime.

• Encouragement of special tribunals and courts to create special cybercrime courts or tribunals with distinct prosecutors and judges and to furnish technical support and speedy procedures to efficiently address complicated cases.

By enacting these legal reforms India can enhance its power to prevent cybercrime and make India a secure digital nation. India enacted Information and Technology Act 2000 and its amendments have given a legal platform to criminals in a variety of cyber offenses from hacking and data theft to online fraud etc. US enacted The Computer Fraud and Abuse Act 1986, UK enacted The Computer Misuse Act, Singapore enacted The Cybersecurity Act.

Important Case Laws decided under Information And Technology Act , 2000 (India):

1. ***Shreya Singhal v. Union of India (2015):*** In this case Supreme court gave the judgment declaring section 66A Unconstitutional. Section 66A of Information Technology Act, 2000 made messages deemed by the police to be offensive and menacing to anyone, or those that caused “annoyance” a criminal offense if these were sent through a computer or computer resource. I t prescribed a prison terms of up to 3 years on conviction. In a PIL filed by Shreya Singhal in 2015, the Supreme court declared section 66A of IT Act,2000 as being violative of article 19(1)(a) of constitution and not saved under the ambit of reasonable restrictions defined in Article 19(2). It had also said that the expressions used in Section 66A were open-ended, undefined and therefore arbitrary. The definition of offense under this section was vague. It was so broadly defined that it took into its sweep protected speech also, and, therefore, upset the balance between the exercise of the right of free speech and the imposition of reasonable restrictions on it. Still, the police used the penal section to deprive the writers on social media of their freedom.

2. ***State Of Tamil Nadu v. Suhas Katti (2004) :*** *(First Conviction under IT Act for cyberstalking and cyber defamation cases)* This case was the first to be filed under Section 67 of the Information Technology Act of 2000, bringing to light the ramifications of publishing pornographic content and saying that any offender, even cyber criminals, cannot be exempted from his/her responsibility. This case was resolved in just 7 months because to the remarkable efficiency of the Chennai Cyber Cell, which is significant in and of itself given the urgent need for a rapid resolution to the issue. This case encouraged several women to come out and discuss the same issues they were facing since, prior to this case, it was embarrassing for the women to discuss the harassment they were experiencing in public. People have been made aware that their legal rights may also be protected online and that they should have trust in the legal system.

   The court's introduction of the validation of a person as a "expert" and the admission of electronic evidence under section 65B of the Indian Evidence Act is the case's most significant development.

   Following this case, which still has a lot of relevance today, "forgery" of electronic evidence, was also recognised as a felony.

3. ***K.S. Puttaswamy v. Union of India (2017) :*** *(Landmark Judgment by 9-Judge-bench of Supreme Court) (**upholding the fundamental right to privacy under Article 21 of the constitution of India**.)*

   It is stated in the judgment that the privacy is to be an integral component of Part III of the Indian Constitution, which lays down the fundamental rights of the citizens. The Supreme Court also stated that the state must carefully balance the individual privacy and the legitimate aim, at any cost as fundamental rights cannot be given or taken away by law, and all laws and acts must abide by the constitution. The Court also declared that the right to privacy is not an absolute right and any invasion of privacy by state or non-state actor must satisfy the triple test i.e.

   1. Legitimate Aim
   2. Proportionality
   3. Legality

   Decision that has been passed by all nine judges holds:

   (i)The decision in ***M P Sharma vs. Satish Chandra*** which holds that the right to privacy is not protected by the Constitution of India stands over-ruled;

   (ii) The decision in ***Kharak Singh vs. State of UP*** to the degree that it holds that the right to privacy is not protected by the Constitution also stands over-ruled;

   (iii) The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the constitution of India and as a part of the freedoms guaranteed by Part III of the Constitution.

VII. DATA PROTECTION ACTS:

The data protection acts is a legislation aimed at the protection of personal data and making sure that it is treated responsibly and securely by organizations. Various nations have individual versions of data protection laws, but the most popular include:

1.The UK Data Protection Act 2018: This is the implementation in the UK of the General Data Protection Regulation (GDPR) and it regulates the processing, storage and transfer of personal

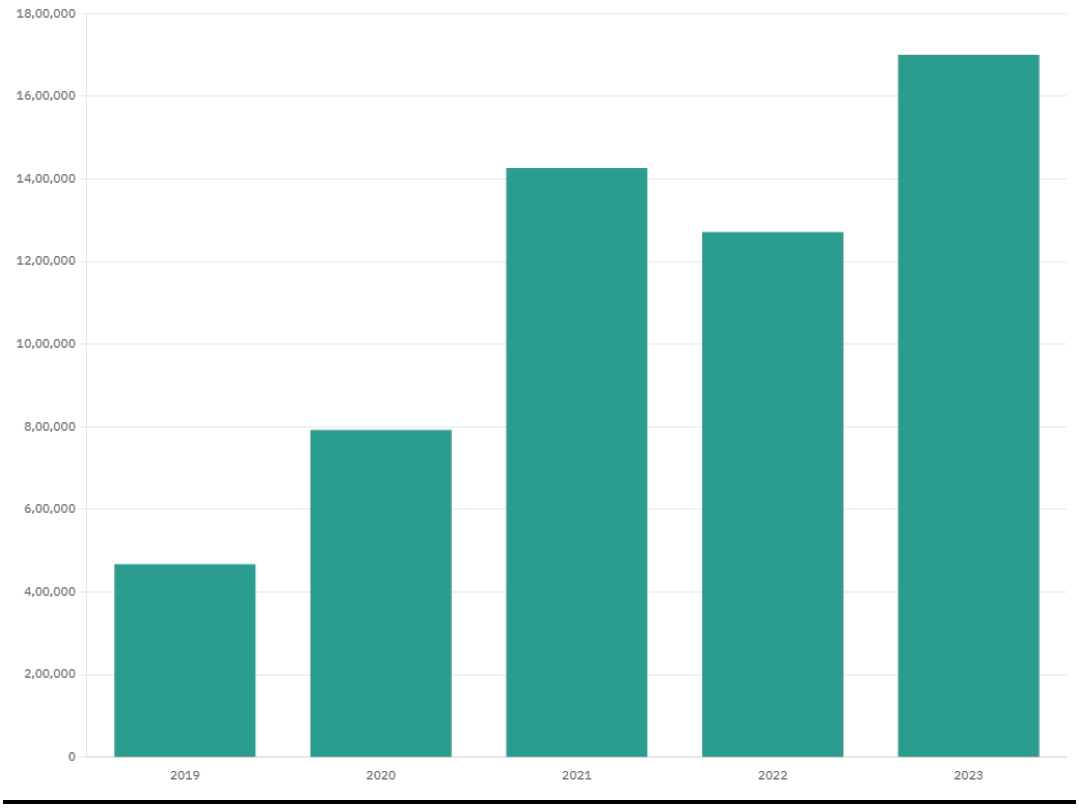
data. It protects individuals' control over their personal data, and it defines the rights of individuals, including the right to access, rectify, and erase data.

2.The UK Data Protection Act 1998: This was the precursor to the 2018 Act. It was significantly superseded by the 2018 Act, although it established the basis for the protection of the personal data prior to the advent of the GDPR.

3.General Data protection Regulation (GDPR): Technically an EU regulation but with a global reach, GDPR is a primary framework for data protection in Europe that has shaped data privacy legislation in other nations. GDPR aims to promote respect for individuals' privacy and make organizations transparent about their data collection and processing activities.

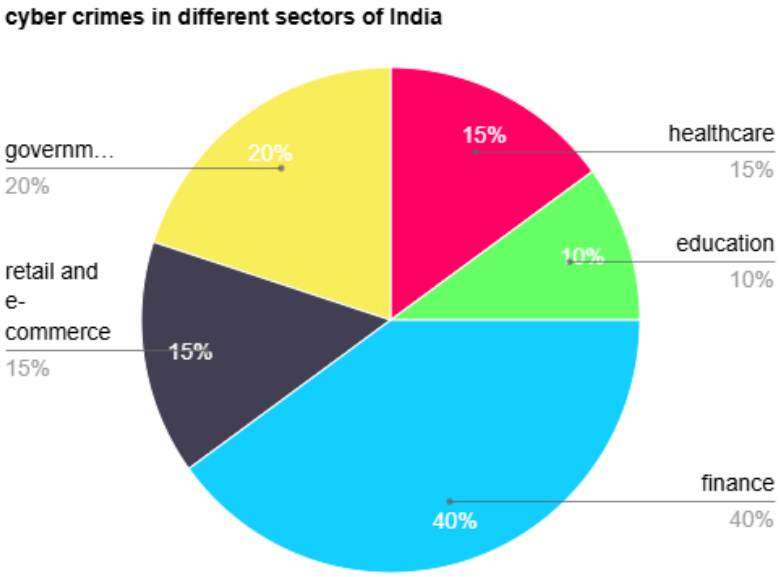
4.Data Protection Act 2003: Refers to a specific legislative act in Jamaica regulating the collection, use, and storage of personal data. This Act was aimed at safeguarding individual's privacy and ensuring that their personal information is dealt with responsibly by organizations and the government.

VIII. CYBER CRIMES 2019-2023 :



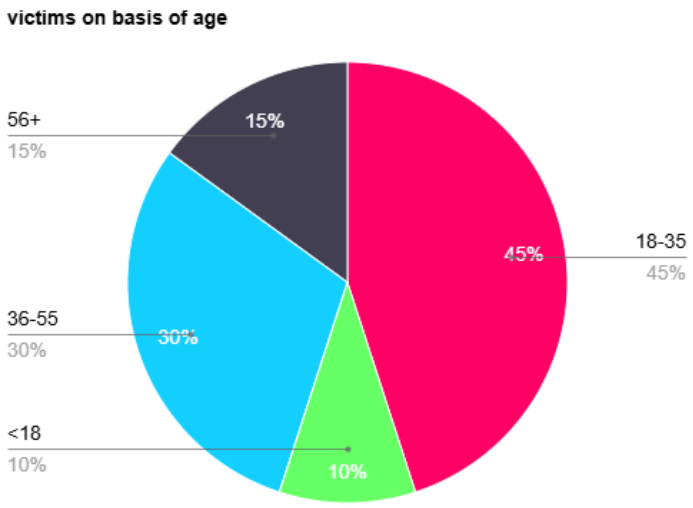
From above Bar Graph we can see that there is a significant increase in cases related to cybercrime from year 2019 to 2023 and with the increase in number of cybercrime cases there is also significant increase in amount of global damages and financial losses each year from 2019 to 2023. To stop these cybercrimes and to stop these financial and global damages every country has implemented data protection acts.

Cyber crimes in India in different sectors -



So, we can conclude that there is highest rate of cybercrimes in finance sector but the healthcare sector is nowadays becoming the primary target for cybercrimes as it contains personal information of people.

Kinds of victims being targeted (on basis of age)–



By the above drawn pie chart we can easily conclude that the highest number of victims that are targeted for cybercrimes are between the age group of 18 to 35.

* RBI Recent Statements Regarding Loss Incurred Due to Cyber Crimes in Fiscal Year 2024:

• During the half-year period in the fiscal year 2024 (April to September), the Reserve Bank of India (RBI) stated that bank fraud cases increased tremendously with 18,461 instances valuing ₹21,367 crore.

• Online scams, both internet and card-based, covered 44.7% of the amount defrauded and 85.3% of the total cases reported during this time.

• To address the increasing cyber threats, the RBI has launched exclusive domain names—'bank.in' for banks and 'fin.in' for financial companies that are not banks—to increase the genuineness of financial websites and curb phishing scams.

• Moreover, the RBI has stressed that awareness regarding cyber frauds and detection of mule accounts is crucial to safeguard consumers as well as the financial system.

Such steps are meant to enhance the resilience of India's financial infrastructure in the face of the mounting danger posed by cyber crimes.

IX. CONCLUSION :

As we navigated the intricate terrain of AI and Privacy legislation, it is apparent that the future necessitates a fine balance between technological advancements and the protection of individual data. AI presents unprecedented capabilities to improve human rights, ranging from improving access to education and healthcare to ensuring social justice and equality. Nevertheless, the moral ramifications of AI algorithms, the danger of privacy invasions, and the possibility of job loss require stringent attention.

Transparency and explainable AI come out as a key determinant in overcoming these problems. With transparency and explainability in AI decision-making, we can protect human dignity and agency. Ethical AI development and utilization through responsible principles and guidelines can result in AI systems that promote and respect human rights and privacy regulations.

A balance between innovation and privacy requires robust legal and regulatory frameworks at national and international levels. Governments, AI builders, civil society, and academia need to work together in designing a human centered future of AI.

In this venture, maintaining data protection and making privacy laws adhere to avoid any form of cybercrime or cyber fraud is key. Encouraging an educated society that understands the possibilities of AI and how it affects human rights of data protection under the guidance of privacy laws empowers people to take part in the decision-making processes that define our shared digital future.

Finally, the onus is on us, being the custodians of AI technology, to guide it in a manner consistent with our common values and hopes. Through the adoption of the principles of fairness, transparency, and accountability, we are able to achieve the fine line between AI innovation and ensuring that the basic rights of humanity in the digital world are secured in the protection of data and for upholding the privacy legislation in protecting the data as because at present there is a high likelihood of becoming the victim of cybercrime if our essential data is not being protected and kept confidential.

X. REFERENCES :

1) The Information Technology Rules 2011(India).

2) The Personal Data Protection Bill,2019(India).

3) The Draft Data Protection Bill,2022(India).

4) The National Strategy on Artificial Inteligence,2018(India).

5) NITI Aayog’s Discussion Paper on AI for All(India).

6) TRAI’s Report on Privacy and Data Protection (2019).

7) Artificial Intelligence and the law” by Thomas D. E. Weiss.

8) www.manupatrafast.in

9) Indian Kanoon. org

10) OECD Report on AI and Data protection.

11) "AI, privacy, and Data protection: Risks and Mitigation Strategies "by global privacy assembly.