"Navigating the Ethical Landscape: Right to Privacy in the Age of AI"

Dr Sakuntala Gouda

Assistant Professor, Capital Law College

DOI: https://dx.doi.org/10.47772/IJRISS.2024.808012

Received: 29 June 2024; Revised: 15 July 2024; Accepted: 20 July 2024; Published: 26 August 2024

ABSTRACT

The fundamental rights were included in the constitution because they were considered essential for the growth of the personality of every individual to preserve human dignity and liberty, such are freedom of speech, expression movement, residence, trade and occupation protected by the State because they were considered essential for the development of the personality of every individual. Right to life guaranteed under Fundamental Rights article 21 of the Constitution of India, is not merely a fundamental right, it includes right to life and personal liberty which are most precious, sacrosanct inalienable and fundamental of all the fundamental rights of citizens which also assure, right to privacy. Right to privacy which are the most essential and basic human rights in a democratic form of government. In our increasingly digitized world, the intersection of artificial intelligence (AI) and the right to privacy has become a paramount concern. The right to privacy, a fundamental human right, faces unprecedented challenges in the wake of AI advancements, like personal data, questions about consent, transparency, and individuals' privacy. This research paper seeks to unravel the intricate relationship among all these realms, exploring the ethical dimensions that arise as AI technologies permeate various aspects of our lives. Furthermore, our discussion will extend to the ethical responsibilities of AI developers, policymakers, and users, will gain insights into designing AI systems that prioritize privacy, emphasizing the need for ethical considerations throughout the development life cycle. A responsible and privacy-centric approach to AI deployment. This seminar paper seeks to unravel the intricate relationship among all these realms, exploring the ethical dimensions that arise as AI technologies permeate various aspects of our lives. The right to privacy, a fundamental human right, faces unprecedented challenges in the wake of AI advancements, like personal data, questions about consent, transparency, and individuals' privacy. The methodology of the study is the descriptive analysis of doctrinal research and based on secondary sources like book, journal. articles and case laws

Key Word: Data privacy, Artificial Intelligence (AI), Personal data, Rights, Digitized world

INTRODUCTION

The last few years of the 20th Century saw rapid strides in the field of science and information technology. The twenty-first century filled with many new gadgets and technological innovations. With the passing of each moment unknowingly, our lives are becoming more and more digitized. Many new technological innovations are rapidly being introduced into this generation. Large majorities of people were embracing all the new gadgets coming into the market because things are becoming more convenient and less time consuming. With a majority of people welcoming the technology and the advancements it brings, such as the usage of telephone calling, automatic teller machines (ATMs), a fully paperless society is on the horizon. As time passes, our lives will become more and more digitized, still we have a name, with a special signature, code, or number may also help to positively identify us.[1]However, convenience and efficiency which tend to also, brought an increasing vulnerability, affecting an individual's identity, privacy and integrity and create conflict of interests. Further, the growth of electronic commerce has created the need for vibrant and effective regulatory mechanisms, which would further strengthen the legal infrastructure that is crucial to the success of electronic commerce.

Artificial Intelligence (AI) is a rapidly advancing field with immense potential to revolutionize various

industries and aspects of our daily lives. It encompasses technologies that simulate human intelligence and decision-making processes, allowing machines to learn, analyse data, and perform tasks autonomously. The development and application of AI have been furled by advancements in machine learning, deep learning, natural language processing, computer vision, and robotics.

AI offers a wide array of benefits, including increased efficiency and automation, enhanced data analysis and insights, cost reduction, improved decision making, and innovative products and services. It has significant applications across industries such as healthcare, finance, automotive, retail, marketing, agriculture, education, and cybersecurity. AI's ability to drive personalized experiences, predict outcomes, and optimize processes has transformed how businesses operate and interact with customers.

This research paper seeks to unravel the intricate relationship among all these realms, exploring the ethical dimensions that arise as AI technologies permeate various aspects of our lives. The right to privacy, a fundamental human right, faces unprecedented challenges in the wake of AI advancements, like personal data, questions about consent, transparency, and individuals' privacy Furthermore our discussion will extend to the ethical responsibilities of AI developers, policymakers, and users, will gain insights into designing AI systems that prioritize privacy, emphasizing the need for ethical considerations throughout the development life cycle. A responsible and privacy-centric approach to AI deployment. The right to privacy, a fundamental human right, faces unprecedented challenges in the wake of AI advancements, like personal data, questions about consent, transparency, and individuals' privacy.

METHODS OF STUDY

The methodology of the study is the descriptive analysis of doctrinal research and based on secondary sources of data like (book, e books, academic literatures in the form of articles, reports by government and nongovernment organisation and case laws. This paper fucuses on holistic approach towards understand the problem between two variables AI and Right to privacy. The study suggested need of global framework to cope with these difficulties and also rigorous judicial punishment who are not adhere the AI ethical guidelines.

Right to privacy which is not specifically define, despite the lack of a uniform legal definition, many legal experts view privacy as an inherent human right that every individual possesses. It is not contingent upon any charter or instrument. Additional dimensions of privacy include freedom of movement and thought, dignity, secrecy, protection from state monitoring, bodily integrity, personal autonomy, and informational self-determination. The right to privacy, in a nutshell, must be evaluated individually. On a global scale, privacy is protected by strong legislation. People are legally protected from "arbitrary interference" with their privacy, like matter concerning family, home, communication, honour, and reputation according to Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) (1966).

Right to Privacy: An Insight Part III of the Constitution of India, which deals with Fundamental Rights, does not include the Right to Privacy since it was not specifically considered by the framers of the Constitution, Judgment has been handed down after much deliberation, and the concept of privacy has been defined. But the Supreme Court did not address the issue of privacy until 1954, a mere four years following the framing of the Constitution. The Supreme Court sided with the search and seizure procedure in the MP Sharma vs Satish Chandra case, which pitted it against the right to privacy. Although the right to privacy is not a constitutionally protected right, the Supreme Court sided with the police in 1962 in Kharak Singh vs. State of UP (AIR 1963 SC 1295), which dealt with the authority of police monitoring in relation to history sheeters. In the history of the right to privacy in India, year 1975 was a turning point.

In the case of Gobind vs. State of MP & ANR [1975 SCC(2) 148], the Supreme Court of India adopted the compelling state interest test, which originated in American law. A compelling broader state interest must supersede an individual's right to privacy, according to the court. The scope of privacy has grown over the years to encompass more types of personally identifiable information, including health records and biometric data. A person's right to privacy in relation to the substance of their telephone conversations was firmly established by the Supreme Court in the landmark 1997 decision of PUCL vs. Union of India, also referred to

as the telephone tapping cases. It follows that the right to privacy was being acknowledged in a number of circumstances, with proper regard also given to its limitations. Aadhaar is a government programme that has been at the focus of privacy debates since the turn of the millennium. Under this plan, individuals are given unique identification cards after providing biometric data (such as fingerprints scan) and demographic information. The Supreme Court issued an order in September 2013 limiting the use of Aadhaar, saying that it should only be used in the public distribution system and for LPG subsidies after it was challenged in court for violating privacy. There was an amendment to the order in October 2015 that stated Aadhaar could be used to provide services like the Mahatma Gandhi National Rural Employment Guarantee Act (MNREGA), the Pradhan Mantri Jan-Dhan Yojana, pension and provident fund schemes, and that no one should be denied a service because they did not have Aadhaar.

Constitutional Aspect The right to personal privacy is enshrined in the right to life and liberty as protected by Article 21 of the Constitution of India which has been taken to mean the right to privacy. Article 21 in context of right to privacy must be interpreted in conjunction with the freedom to publish any subject of public interest, within reasonable limits, as guaranteed by the Constitution.

With a constitution that incorporates the ideas of justice, liberty, equality, and fraternity, India set off on its constitutional journey in 1950. The country is known for its cultural variety and rich traditions. Without being specifically mentioned, the right to privacy is inextricably woven into the fabric of our constitution, since it is guaranteed under Articles 19 and 21 dealing with the evolution of the right to privacy in Indian law, including significant decisions that helped establish the right as an inherent and unalienable one. Many facets of privacy law and its basis in theory thoroughly investigate the structure that control privacy in India, including statutes, court rulings, and treaties. Particularly, it analyses seminal decisions made by India's highest court, such the Puttaswamy case, which dealt with the complex relationship between personal data protection in the digital era and firmly upheld the rig to privacy as a basic human right. [2]

APPLICATIONS OF ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence (AI) has a vast range of applications across various industries and domains. Its ability to simulate human intelligence and automate complex tasks makes it a valuable tool for improving efficiency, accuracy, and decision-making. Here are some prominent applications of AI:

1.Healthcare: Medical Diagnosis: AI can analyze medical imaging (e.g., X-rays, MRIs) to assist in diagnosing conditions like cancer, fractures, and other ailments

2. Drug Discovery: AI accelerates drug development by predicting molecular behaviour and potential drug interactions, leading to faster and more efficient drug discovery. [3]

3. Personalized Medicine: AI analyzes patient data to tailor treatment plans and drug dosages for individual patients, optimizing healthcare outcomes.

4. Finance: Fraud Detection: AI algorithms can detect unusual patterns in financial transactions to identify potentially fraudulent activities and enhance security. Risk Assessment: AI helps assess investment risks and forecast market trends by analysing historical data, enabling better-informed investment decisions.

5. Customer Service: AI-powered chatbots provide customer support, handle queries, and offer assistance with banking transactions, improving customer experiences.

6. Automotive: Autonomous Vehicles: AI enables self-driving cars by processing data from sensors and making real-time decisions to navigate and drive safely without human intervention.

7. Predictive Maintenance: AI predicts when vehicle components might fail, optimizing maintenance schedules and reducing downtime

8. Retail: Personalized Shopping: AI analyses customer behaviour and preferences to offer personalized product recommendations, enhancing the shopping experience. Stockouts.

Previous studies[4]

RISKS OF ARTIFICIAL INTELLIGENCE

(AI) Artificial Intelligence (AI) brings transformative potential, but it also comes with several risks and challenges that need to be carefully managed. Here are some of the key risks associated with AI:

1. Bias and Fairness: AI models can inadvertently learn biases present in the training data, leading to biased outcomes in decision-making and reinforcing existing cultural biases. Bias can manifest in AI systems related to gender, race, age, socioeconomic status, and other factors, resulting in unfair treatment and discrimination.

2. Lack of Transparency and Interpretability: Deep learning models, in particular, can be complex and difficult to interpret, making it challenging to understand how they arrive at specific decisions or predictions. Lack of transparency can hinder trust and acceptance, especially in critical domains like healthcare, finance, and legal systems.

3. Data Privacy and Security: AI relies heavily on data, and the collection, storage, and use of vast amounts of personal data raise concerns about privacy violations and unauthorized access to sensitive information

4. Malicious actors may attempt to manipulate or misuse of AI systems, posing a significant threat to individuals, organizations even if national security and privacy system.

5. Job Displacement and Economic Impact: As AI automation advances, there is a risk of job displacement, particularly for routine and repetitive tasks, potentially leading to unemployment and economic disruption in certain sectors. Job displacement may affect low-skilled workers, necessitating the need for workforce retraining and upskilling.

6. Autonomous Weapons and Ethical Concerns: The development of AI-powered autonomous weapons raises ethical questions about the potential for misuse, loss of human control, and compliance with international laws and ethical standards in warfare.[5]

The evolution of information technology gave birth to the Space. Cyber space is a very wide term and includes computer networks, software, data storage devices (such as hard disks, disks etc), the Internet, websites, e-mails and even electronic de such as cell phones, ATM machines etc. It is governed by a system law and regulation called cyber law. In today's highly digitalized w cyber law affects almost everyone. Cyber law can be defined as the law governing computers and the internet. It encapsulates the legal issues related to use of to communicative, transactional and distributive aspects of networked conformation devices and technologies in general.[6]

E-governance

The World Bank defines e-governance as the use of information and communication technologies by government agencies to transform relations with citizens, business world and other arms of the government. In India, ever since the creation of Ministry of Information Technology in the Union Government, State and Union Territories expressed commitment for providing effective, responsive and transparent citizen governance through the use of Information Technology. E-governance is used as a synonym for an Information Technology driven system of governance that works better, costs less and is capable of servicing people's needs.

Confidentiality & Privacy

There have been instances where MMS clips have been shot and circulated on the internet. For instance, a MMS clip was shot by a Delhi schoolboy" and circulated on Bazee.com, leading to the arrest of its Chief Executive Officer of American origin. Section 66E has now been introduced under the IT Act 2000 for the protection of physical or personal privacy of an individual. This section makes intentional capturing of the images of a person's private parts without his or her consent in any medium and publishing or transmitting

such images through electronic medium, a violation of such person's privacy punishable with imprisonment of up to three years or with fine up to Rupees Two Lakhs, or both.

Cyber Pornography

There is no settled definition of pornography or obscenity, which were considered simply sexually explicit but not obscene in USA, that can be considered obscene in India. There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect. Pornography on the Internet is available in different formats, These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is unconstitutional, The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive. Such Acts are covered by Section 67 of Information Technology Act. Section 67 of the IT Act is the most serious Indian law penalizing cyber pornography. Other Indian laws that deal with pornography include the Indecent Representation of Women (Prohibition) Act and the Indian Penal Code.[7]

According to Section 67 of the IT Act, whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter mut contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupee.

Deepfake AI

Deepfake AI involves using artificial intelligence to create manipulated or synthetic content, often in the form of realistic-looking videos or images where the subjects appear to say or do things they never did. In the context of privacy rights under Article 21 of the Indian Constitution, deepfake AI can be considered a threat as it can be used to fabricate content that invades an individual's privacy.

Article 21 of the Indian Constitution protects the right to life and personal liberty. Deepfake AI could infringe upon this right by creating misleading content that harms an individual's reputation, dignity, or personal relationships. Although there might not be specific cases directly addressing deepfake AI in Indian courts

Cyber Squatting

One eminent problem in the cyber space is cybersquatting, which leads to the infringements of the rights of others in terms of trademarks. It has been defined as "deliberate bad faith registration as domain of well-known trademarks in the hope of being able to sell the domain to the owners of those marks (or rivals owners) or simply to take unfair advantage of the reputation attached to those marks. It is a cyber offence adversely affecting the trading companies as due to the registration of their trademarks by any other person with malafide intention, the companies have to either enter into an unreasonable bargaining or they have to enter into a legal action which they often, due to the unavailability of stringent and particular laws in this regard, lose. Cyber Tons of squatting does not take place only with regard to the trademarks of the companies but it can also occur in cases where the name of an eminent personality is used as the domain name by any other person. In this age of e-commerce it is very significant for the companies to have their websites by the names of their trademarks. Often when the company wants to have its own website by the name of its trademark.

In India Cyber law is largely governed by the Information Technology Act 2000 Cyber law encompasses laws relating to Cyber Crimes, mainly focuses on Electronic and Digital Signatures. Intellectual Property Rights, E-governance, E-commerce The primary offences under the IT Act were: Tampering with source code-Deleting, destroying or altering any data on any computer resource with mala fide intent to cause wrongful loss or to diminish value ,Publishing or transmitting pornographic material through computer resource Provisions pertaining to encryption technology, the right the Government Authorities to intercept and decrypt such data and call upon any entity or individual to decrypt such data were also included in the IT Act. Certain Acts

affecting the integrity and sovereignty of the nation were classified as offences. The ITAA 2008 added eight offences, five of which are added to the IT Act 2000 and three to IPC. The new offences are as follows:

Section 66, combines contraventions indicated in Section 43 with penal effect and reduces the punishment from 3 years to 2 years. It also introduces the pre-conditions of "Dishonesty" and "Fraud" to Section 66.

Section 66 A, covers Sending of Offensive messages. Section 66B is a new section added in the ITAA 2008, which states, 'whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe that the same to be a stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. This section appears to cover theft of computer laptop, mobile and also information. It can be extended to theft of digital signals of TV transmission sec Section.43 , sec 65, sec 66 of the IT Act. Section 65 of the IT Act.

Section 66 misleadingly termed "Hacking" under the IT Act Section 66 C, is a new section added in the ITAA 2008 which states 'whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term that extends up to three years and shall also be liable to fine which may extend to rupees one lakh' This section covers password theft which was earlier being covered under Section 66.

Section 66 D ,is a new section added in the ITAA 2008 which states, whoever by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees'. This section covers Phishing which was earlier being covered under Section 66. It may also cover some kinds of e-mail related offences including harassment. and Section 66 E is a new section added in the ITAA 2008 which states 'whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that persons, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or with both.The amendments introduced to the Information Technology Act, 2000, notified through the Jan Vishwas (Amendment of Provisions) Act, 2023, came into effect on Thursday (November 30). Five offences have been decriminalised, while penalties for two others have been increased.

7. Data Protection and Privacy Cybercrimes are unlawful acts where the computer is used either as a tool or a target or as an accessory to store illegal or stolen information. The enormous growth in electronic commerce (e- commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime, Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

8. Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements: signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures. Intellectual property refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law. These include:

1. copyright law in relation to computer software, computer source code, websites, cell phone content etc, 11) software and source code licenses111) trademark law with relation to domain names, meta tags, 1V) semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts, mirroring, framing, linking etc V) patent law in relation to computer hardware and software

Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements: signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures. Intellectual property refers to creations of the human mind e.g. a

story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law. These include:

1. copyright law in relation to computer software, computer source code, websites, cell phone content etc, 11) software and source code licenses111) trademark law with relation to domain names, meta tags, 1V semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts, mirroring, framing, linking etc V patent law in relation to computer hardware and software

Modern privacy concerns are fuelled by the ever-present digital surveillance state, massive data collecting, and lightning-fast technology developments. these difficulties, elucidating the consequences for personal freedoms and privacy. At a time when the confidentiality of individual data is under grave danger, this incident highlights the critical need for strong legislative provisions and safeguards. The ever-changing notion of personal privacy guaranteed by the Indian Constitution—a notion that speaks to the hopes and dreams of a contemporary, digital India. Reiterating the Constitution's dedication to protecting individual rights, it encompasses the values of human autonomy, dignity, and liberty. [8]

An important issue is the jurisdiction in cybercrimes. A crime in one country may not be treated as a crime in another country. The Jurisdiction issue relates to the fact that online crimes can extend to other towns, counties, cities, states or even countries. It may sometimes be uncertain as to whether such an investigation should be handled by the local agency that initially took the complaint, which eventually led to an investigation. If a crime is transnational which law can be applied?

Jurisdiction over cyber crimes should be standardized around the globe to make swift action possible against terrorists whose activities are endangering security worldwide. Differences in the laws among countries prevented effective investigation against cyber terrorism, which is not bound by national boundaries, and each investigation could involve several countries.

Global Mechanism to Control Cyber Crimes

In any field of human activity leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is stringent as according to its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe.

The amendments introduced to the Information Technology Act, 2000, notified through the Jan Vishwas (Amendment of Provisions) Act, 2023, came into effect on Thursday(November30). Five offences have been decriminalised, while penalties for two others have been increased. Amendments to different acts will come into force through notifications by respective administrating ministries .

India’s approach to AI is substantially informed by three initiatives at the national level, The first is Digital India, which aims to make India a digitally empowered knowledge economy. The second is Make in India, under which the Government of India is prioritising AI technology designed and developed in India, and the third is the Smart Cities Mission (Marda 2018).

Alongside this, there is significant investment towards research, development and training in emerging technologies in particular from the Union Government. An AI Task Force constituted by the Ministry of Commerce and Industry in 2017 looked at AI as a socio-economic problem solver at scale. In its Report (Government of India Ministry of Commerce and Industry 2018) it identified 10 key sectors in which AI should be deployed, including national security, financial technology, manufacturing and agriculture, among others.

Similarly, a National Strategy for Artificial Intelligence was published in 2018 (Niti Aayog 2018) that went further to look at AI as a lever for economic growth, social development, and considers India as a potential ‘garage’ for AI applications. While ethics are mentioned in both documents, they fail to meaningfully engage

with issues of fundamental rights, fairness, and the limits of data driven decision making. These are also heavily influenced by the private sector, with civil society and academia rarely, if ever, being invited into these discussions. AI is being used in various sectors by private actors - from manufacturing, to healthcare, to finance.

Notwithstanding encouraging developments, the current absence of data protection legislation in India raises crucial questions for how sensitive personal data is currently processed and shared. The current Personal Data Protection bill also fails to adequately engage with the question of inferred data, which is particularly important in the context of machine learning. wIndia's biometric identity project, Aadhaar, could also potentially become a central point of AI applications in the future, with a few proposals for use of facial recognition in the last year, although that is not the case currently. There is no ethical framework or principles published by the Government at the time of writing. It is likely that ethical principles will emerge shortly, following public attention on data protection law. Current references to AI are often in the context of data protection law, which is an increasing trend across jurisdictions means, which countries have power to deals with this offences, which countries can hold the power of retract the sources if any ethical issues arises, till now certain offences which were proceeded through AI untouched.

CONCLUSION AND SUGGESTION

Growth and development of in the field of Industrial sector, urbanisation, trade and commerce, information technology, social networking site and communication through internet is important facet of this digital world, IT has made social and workplace interaction convenient, cost-effective, quick and The Information Technology made the whole world as 'global village connecting everyone by internet more real. IT has emerged as the powerful means to voice of public opinion and social movements. It serves a powerful tool of communication and facilities civil liberties and democracy campaigns. screening due diligence checks, data mining, restoring and education to negotiating business contracts, tele-medicine, online dispute resolution and varied applications using 'voice over internet protocol technique.

And demand came from various quarters for enactment of proper law so that cyber intrusion may be controlled. The data were available in computers and when the computer is connected with internet, the entire computer system is open to access by the whole world, which exposes all the data, may there be secret data of concerning security and privacy of any person , company and countries ,Cyber Technology has made people too dependent upon the computers and internet despite the danger of being exposed to the entire world and despite the threat of leakage of all the confidential matters ,may be personal or commercial, but there is no way out except to go in pace with the new technology which makes everybody in touch with the entire world with respect to all the developments on in this era of competition and consumerism it is impossible to think of living without computers or internet.

However the right of privacy in the matter of personal life or of a trade and commercial activities is also a valuable right and cannot be permitted to be invaded by anybody, how strong the processes and product may be. Therefore with the advent of Internet privacy involves, the right of personal privacy concerning the storing, repurposing, providing third parties and displaying of information pertaining to oneself via the internet privacy can entail both Personally Identifying Information (PII) or non-PI information such as a State visitor's behaviour on a website. Personally Identifying Information is any information that can be used to identify an individual. For example; age and physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person.

Suggestion

IT law should be need more comprehensive framework and set up a specific regulatory body to cope with this emerging issues of right to privacy and AI, infringement of privacy rights can minimize by employment of privacy-enhancing technologies ,and regular privacy impact assessment should be conducted to identify and address vulnerabilities groups, of this area, such dispute should be handle with care ,privacy ,accountability and transparency should maintain during the proceeding of such dispute ,Ethical guidelines for AI should be strictly adhere with strict judicial mechanism followed with rigorious punishment.

User must strictly control over their data and also control data security ,including access and deleting the information. which can minimize this threat ,fostering the users rights obligation towards the society can be enhance through the public awareness education, which can be minimize the must spreading problems this AI.

REFERENCE

Bibliography Books

1. Bakshi, P.M. & Suri, R.K. Cyber and E-Commerce Laws, Bharat Publishing House, New Delhi, Edn. 1,2002. Computer Evidence and Computer Crime Forensic Science, Computers and The Internet, Cambridge University Press, 2000.
2. Sharma, Dr.B.R. Forensic Science in Criminal Investigation And Trials, Universal Law Publishing Pvt. Ltd, 4th Edn, 2005.
3. almer, James. "Artificial Intelligence and Legal Merit Arguments." PhD Thesis, University of Oxford, 1997. https://ep.nz/s/Artificial-Intelligence-and-Legal-Merit-Arguments_Final-Thesis-d9b9.pdf.
4. "'No Regulations for Artificial Intelligence in India': IT Minister Ashwin Vaishnaw - BusinessToday." Accessed January 18, 2024. https://www.businesstoday.in/technology/news/story/no-regulations-for-artificial-intelligence-in-india-it-minister-ashwini-vaishnaw-376298-2023-04-06.
5. Meskys, Edvinas, Julija Kalpokiene, Paul Jurcys, and Aidas Liaudanskas. "Regulating Deep Fakes: Legal and Ethical Considerations." SSRN Scholarly Paper. Rochester, NY, December 2, 2019. https://papers.ssrn.com/abstract=3497144.
6. Verma, Manish. "Artificial Intelligence Role in Modern Science: Aims, Merits, Risks and Its Applications." *Artificial Intelligence* 7, no. 5 (2023). https://www.researchgate.net/profile/Manish-Verma-47/publication/374188976_Artificial_Intelligence_Role_in_Modern_Science_Aims_Merits_Risks_and_Its_Applications/links/6512d4e64aa1fe047007e05a/Artificial-Intelligence-Role-in-Modern-Science-Aims-Merits-Risks-and-Its-Applications.pdf.
7. Aly, Heidi, 'Digital Transformation, Development and Productivity in Developing Countries: Is Artificial Intelligence a Curse or a Blessing?', *Review of Economics and Political Science*, 7.4 (2020), pp. 238–56 <https://www.emerald.com/insight/content/doi/10.1108/REPS-11-2019-0145/full/> [accessed 26 December 2023]
8. Balamurugan, R., S. Inbakumar, and R. G. Sethuraman, 'A Critical View on the Impact of Constitution of India as Internal Regulatory Mechanism for Environmental Issues and Policies', *Indian Journal of Science and Technology*, 4.3 (2011), p. 263 <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=83f2ef75ab780bcb09cfd37b17263c1aa7331c08> [accessed 6 December 2023]
9. Déchaux, Raphaël, 'Legal Framework on AI: Merits of Different Type of Legal Instruments According to the Principles to Protect or to Promote', in *Hackathon Du Groupe de Soutien Du Comité Ad Hoc Sur l'intelligence Artificielle*, 2020 <https://amu.hal.science/hal-03159688/document> [accessed 26 December 2023]
10. Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, and others, 'An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations', in *Ethics, Governance, and Policies in Artificial Intelligence*, ed. by Luciano Floridi, Philosophical Studies Series (Springer International Publishing, 2021), cxliv, 19–39, doi:10.1007/978-3-030-81907-1_3
11. Khosla, Sunil, 'The Right to Privacy: Constitutional Perspective in India', *Innovative Research Thoughts*, 3.2 (2017), pp. 121–27 <https://irt.shodhsagar.com/index.php/j/article/view/526> [accessed 13 July 2024]
12. Verma, Manish, 'Artificial Intelligence Role in Modern Science: Aims, Merits, Risks and Its Applications', *Artificial Intelligence*, 7.5 (2023) <https://www.researchgate.net/profile/Manish-Verma-47/publication/374188976_Artificial_Intelligence_Role_in_Modern_Science_Aims_Merits_Risks_and_Its_Applications/links/6512d4e64aa1fe047007e05a/Artificial-Intelligence-Role-in-Modern-Science-Aims-Merits-Risks-and-Its-Applications.pdf> [accessed 26 December 2023]

FOOTNOTES

[1] Raphaël Déchaux, 'Legal Framework on AI: Merits of Different Type of Legal Instruments According to the Principles to Protect or to Promote', in *Hackathon Du Groupe de Soutien Du Comité Ad Hoc Sur l'intelligence Artificielle*, 2020 <https://amu.hal.science/hal-03159688/document> [accessed 26 December 2023].

[2] Sunil Khosla, 'The Right to Privacy: Constitutional Perspective in India', *Innovative Research Thoughts*, 3.2 (2017), pp. 121–27 <https://irt.shodhsagar.com/index.php/j/article/view/526> [accessed 13 July 2024].

[3] Déchaux; Heidi Aly, 'Digital Transformation, Development and Productivity in Developing Countries: Is Artificial Intelligence a Curse or a Blessing?', *Review of Economics and Political Science*, 7.4 (2020), pp. 238–56 <https://www.emerald.com/insight/content/doi/10.1108/REPS-11-2019-0145/full/> [accessed 26 December 2023].

[4] Manish Verma, 'Artificial Intelligence Role in Modern Science: Aims, Merits, Risks and Its Applications', *Artificial Intelligence*, 7.5 (2023) <https://www.researchgate.net/profile/Manish-Verma-47/publication/374188976_Artificial_Intelligence_Role_in_Modern_Science_Aims_Merits_Risks_and_Its_Applications/links/6512d4e64aa1fe047007e05a/Artificial-Intelligence-Role-in-Modern-Science-Aims-Merits-Risks-and-Its-Applications.pdf> [accessed 26 December 2023].

[5] Verma.

[6] Verma.

[7] R. Balamurugan, S. Inbakumar, and R. G. Sethuraman, 'A Critical View on the Impact of Constitution of India as Internal Regulatory Mechanism for Environmental Issues and Policies', *Indian Journal of Science and Technology*, 4.3 (2011), p. 263 <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=83f2ef75ab780bcb09cfd37b17263c1aa7331c08> [accessed 6 December 2023].

[8] Khosla.