INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

 ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE: NAVIGATING PRIVACY IN THE ERA OF SIMULATED REALITIES

AUTHORED BY - SHANIKA SHUKLA

Abstract

As we know, AI systems do affect privacy in a variety of ways, just not necessarily in the ways that one may anticipate. The ethical advantage that individuals typically have with regard to information about themselves and the kind of control over information about oneself, that people rely on in regular interpersonal interactions are only two of the elements of privacy that AI systems do threaten. Privacy in itself is really about an interest in how others see us, and AI systems are not capable of forming the kinds of impressions that may potentially conflict with this interest. This paper demonstrate that AI systems do impact privacy in a number of ways, but sometimes not in the manner that one might expect. s, deepfakes are specifically used to disseminate fake information and propaganda on social circles that tarnish the reputation of an individual or an organization. Recently, many surveys have focused on generating and detecting deepfake images, audio, and video streams We must be conscious that the existence of vast volumes of personal data in AI systems does raise the possibility that privacy may be compromised, should a creature with the ability to develop opinions based on that data have that data.

Keywords: Artificial intelligence, Privacy, Deepfakes, Generative adversarial networks.

Introduction

The advent of artificial intelligence and the accompanying technology revolution have completely changed our lives in ways that were previously unimaginable. High-level cognitive functions like thinking, perceiving, learning, problem-solving, and decision-making are now possible because to artificial intelligence (AI), which has brought about development in data collecting and aggregation, analytics, and computer processing power. These technology advancements are now very common and prevalent, affecting every aspect of our life. “The

 ISSN: 2582-6433

"technomy community" has been spawned by the fourth revolution that we are currently seeing"[1]. AI, machine learning, deep learning has made it easier to collect and process large amount of data that provide a wide range of information to us to work from.

Yet we cannot undercut the importance of artificial intelligence or data privacy regulations. However, we shouldn't allow data protection laws and artificial intelligence to undermine each other's usefulness. Instead, machine learning mechanisms should be created that monitor both variables—personal data protection and AI—to ensure that they don't cross over into each other's domains while carrying out their respective intended functions.

Artificial intelligence

Artificial intelligence has a long history of sixty years. It is a set of science, technology that aims to imitate the reasoning and cognitive abilities of a human. As a field of science artificial intelligence included machine learning. Algorithm and deep learning concepts. In the early 1940s and 1950s, research and scholars in engineering, mathematics, computer science explored the possibility of the artificial brains and tried to define and elaborate the concept of machine learning.

In the 1950s, Alan turning, a mathematician and computer scientist published his work "Computer Machinery and Intelligence" which put forward a test of machine learning called "The Imitation Game" through which experts used to measure the ability of machine intelligence to exhibit the human behaviour. The test came to be known as The Turning Test. Later the test was criticized on the notion that machine cannot possess a "mind," or "consciousness" regardless of how much human like program it might make the computer behave.

The term "artificial intelligence" was first coined in 1955 by John McCarthy of MIT (Massachusetts Institute of Technology) when he held his first academic conference on the subject. He defined AI as "the science and engineering of making intelligent machines." It was further explained by the cognitive scientist Marvin Minsky as "the construction of computer programs that engage in task that are currently more satisfactory performed by human beings because they require high level mental processes such as: perceptual leaning, memory organization and critical thinking." In 1956, Marvin in his book "Stormed search for artificial

[1] Sunitha Jain & Simran Jain, Artificial Intelligence: A threat to Privacy, Vol 8, SSRN, (April 17) pp 28

 ISSN: 2582-6433

intelligence" stated that "the problem of artificial intelligence modelling within a generation will be solved". The first artificial intelligence application was introduced during this time which were based on logic theorems and chess games.

In recent years, artificial intelligence (AI) has grown significantly. Today, companies in the public and private sectors worldwide are using artificial intelligence (AI) tools more and more. The potential of AI both now and in the near future offers significant and broad advantages to people, organizations, and society as a whole.

These same technical advancements, however, also bring up significant concerns, such as the conflict between artificial intelligence and data privacy regulations. Because of this, we have a duty and a chance to assess the efficacy of present data protection legislation in light of technical realities of the twenty-first century.

Concept of privacy

Privacy is a universal concept and yet have no concrete definition of its own. It has always differed according to the prevailing societal norms, economy, and cultural environment. Due to this privacy must be interpreted considering the current era and context. "Three layers have been identified by American law professor Alan Westin as influencing privacy norms: the political, the socio-cultural, and the personal"[2]. "Additionally, the individual is crucial: privacy may be thought of as a kind of "aura" that surrounds the individual, which is what separates him or her from the outside world"[3]. "Suggesting changes in the definition of privacy that give exact view of the nature of privacy, Daniel Solove created six categories of privacy"[4].

- "The right to be alone."
- "Limited access to the self"
- "Secrecy,"
- "Control of personal information"
- "Personhood"
- "intimacy"

[2] Westin, A.F.: Social and political dimension of privacy, Journal of Social issues, Vol 59, No.2 (2003) pp. 431-434
[3] Adrienn Lukacs, what is privacy? The history and Definition of Privacy, Sem. Sch, 2016, pg. 258
[4] Ibid

 ISSN: 2582-6433

In international law, People are legally protected from "arbitrary interference" with their privacy, family, home, communication, honor, and reputation by Article 12 of the 1948 Universal Declaration of Human Rights and Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR). Worldwide, the right to privacy has become a fundamental human right. In India, this right is enshrined in article 21 of the Indian Constitution.

Challenges of privacy

AI's speed, size, and automation have made it highly desirable. Artificial intelligence (AI) can currently do computations at a pace quicker than human analysts, and it can be made even faster by adding new technology. AI is perhaps the only method to analyse huge data in a small duration of time since it is naturally skilled at using enormous data sets for analysis. Ultimately, the analytical efficiency is significantly increased when an AI can carry out the assigned duties without supervision.

Deep fakes

Deep fakes are synthetic media that uses Artificial Intelligence to manipulate or generate, audio and visual, usually with the intention of deceiving or misleading people. Synthetic media means any media which has been moulded or modified or manipulated through the use of Artificial Intelligence, especially if done in an automated fashion. In other words, a deep fake is a video or audio or photo that seem real but has been manipulated with the use of AI. The underlying technology can replace figure, manipulate facial expression, synthesize faces and speech. Deep fakes can depict someone is appearing to say or act something that they in fact never said or did. “Cheap fakes” are another version of synthetic media in which simple digital techniques are applied to content to alter the observer’s perception of an event. Cheap fake examples described elsewhere in this paper demonstrate speech being slowed, and video being accelerated. Science and technology are constantly advancing. Deepfakes, along with automated content creation and modification techniques, merely represent the latest mechanisms developed to alter or create visual, audio, and text content.

Deepfakes are strong tool that can be used for exploitation and misinformation. Deepfakes could influence election and erode trust but so far have mainly been used for non-consensual Pornography and defaming content. The underlying artificial intelligence technologies are widely available at lower cost and improvements makes the deep fakes harder to detect.

 ISSN: 2582-6433

Types of deepfakes

The manipulated content can be of any form that has its own challenges while detecting them correctly and the risk of damage that it can do to an individual/organization. Various deepfakes generate manipulated content with diverse approaches. Deepfake content can be categorized as

- Speech produced by AI or manipulated by AI to sound real is known as audio deepfake.
- Text deepfake refers to any text on the internet or in media that has been artificial intelligence (AI) created or altered to appear authentic.
- Video deepfakes: Videos that have been altered, synthesized by AI, in which a person's face is replaced, their body is reenacted, or the speech pattern is changed—all constitute video deepfakes.
- Image deepfake: A deepfake picture is one that has been artificially altered, synthesized, and/or face swapped. It is mostly produced using generative adversarial networks.

Although image and video deepfakes can be of the same category as image deepfakes, where the frame-by-frame manipulate video content are essentially images. There are deepfakes that manipulate audio as well as video content altogether to create lip-sync videos. "Although for image and video manipulations, there exist different techniques. For creating image and video deepfakes, majorly face manipulations have been preferred. For face manipulation, there are multiple diverse types of manipulations possible, which are categorized as entire face synthesis, identity swap, attribute manipulations, and expression swap. Although full-body puppetry can also be seen in deepfakes manipulated videos. Full body puppetry means the movement of a person's body is transposed over another person's body"[5].

How deepfakes works

The image and the videos can be modifying and manipulated by using two major DL model, i.e., autoencoder and GANs. These two are driving force for deepfakes generation.

Autoencoders

"A subtype of feedforward neutral network plays an important role in the creation of deepfakes. Designed by Geoffrey Hinton in the 1980s, autoencoders duplicate input data from the input layer

[5] Sundeep Tanwar et al., Deep fakes Generation and Detention Case study and Challenges, Vol 11, Res.Gate., 143296, 143306, (2023).

 ISSN: 2582-6433

to the output layer, aiming to reconstruct the original input as accurately as possible"[6]. These neural networks consist of an encoder, a code, and a decoder, facilitating the transformation of input data into a compact representation before decoding it to generate the reconstructed output. Deep autoencoders, with multiple layers have encoding and decoding, enable the compression and dimensional reduction of images, a crucial step in deepfake creation.

Generative Adversarial Network

"Generative Adversarial Networks (GANs) includes a powerful class of deep neural networks. Generative Adversarial Networks (GANs) have of two neural network models: a generator and a discriminator. GANs operate in an adversarial setting to generate synthetic data resembling real data distributions. These models are trained concurrently using adversarial training, in which the generator attempts to produce realistic data samples to deceive the discriminator, while the discriminator tries to distinguish between real and fake data samples.

As training progresses, both models improve iteratively, with the generator producing more realistic samples and the discriminator becoming more adept at distinguishing between real and fake samples. This competitive process enables GANs to capture and replicate the variations found in the training dataset, producing high-quality synthetic data that closely resembles the original dataset"[7].

Cases Of Deep Fakes

Deepfake are becoming a serious threat to people in tis digital era. There have been numerous cases of deepfakes that were misleading and offensive.

According to the police, the first among such case in India happened on November 30, when a 76-year-old man was extorted by a criminal through a video call featuring the face and the voice of a retired IPS officer in U.P. Police. The person ended by making repeated payment to the criminal in fear that the police will take action against hi for what apparently looks like him solicitating sex through a video call.

"Another similar case happened in Ghaziabad, wherein a fraudster-initiated contact through a

[6] Dennis Lucky Tuanwi Bale et al., Deepfake detention and classification of image from video: A review of feature, techniques, and challenges, vol 13 (2024)
[7] *Ibid.*

 ISSN: 2582-6433

Facebook video call, flashing a nude pic to trap the person. Sometime later the same person received a video call from a person impersonating the former ADG Prem Prakash who was a senior police officer. The person threatened him to say that they will lodge a criminal case against the person's father. Due to the fear the person deposited 5.000 and later deposited up to 74,000 monies. The case was registered through a complaint received by Integrated Grievance Redressal System (IGRS).

The police said they will write to META, Facebook, and WhatsApp to obtain details of the criminals' account." [8]

"Deepfakes are not only restricted to featuring only one person. A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police".[9]

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

Famous Bollywood celebrity Rashmika Mandana have also been targeted in these deepfakes video. The Delhi Commission for Women (DCW) issued a notification to the city police, and on November 11, 2023, the Intelligence Fusion and Strategic Operations (IFSO) of Delhi Police registered a First Information Report (FIR) against unnamed individuals in connection with the matter.

Ever since the actor's fake video went viral, the government has been very vocal about tackling such cases. On November 24, the IT ministry sent two letters to all social media platforms reminding them of their responsibility to weed out misinformation and deepfakes as mandated by Indian law. "IT minister Ashwini Vaishnaw termed the deepfakes as a "new threat to democracy," adding that the government is working on coming up with new regulations to tackle such situations"[10].

[8] Man Gets caught in deep fake trap, almost ends life, E.T. News, Nov 30, 2023

[9] Heather Chen, finance worker pays out $25 million after video call with deepfake 'chief financial officer'. Feb 4, 2024.

[10] Manjiri Chitre, Rashmika Mandanna deepfake case: Delhi Police track down 4 suspects, hunts for key conspirator on, Hindustan Times (Dec 20, 10:00 AM), https://www.hindustantimes.com/india-news/rashmika-mandanna-deepfake-case-delhi-police-track-down-4-suspects-hunt-for-key-conspirator-on-101703043714888.html

 ISSN: 2582-6433

Prime Minister Narendra Modi raised concerns over the misuse of AI for creating 'deepfakes,' saying that the media can play a role in raising awareness about this crisis. During a "Diwali Milan" event at the Delhi BJP headquarters, Prime Minister Narendra Modi spoke to a group of media members. He said: "A new crisis is emerging due to deepfakes produced through artificial intelligence. There is a very big section of society that does not have a parallel verification system… This (deepfake) will take us to grave danger and has the potential to spread the fire of dissatisfaction."[11]

The PM cited a video he saw recently of him performing garba even though he has not done so since schooldays. "I recently saw a video in which I was playing garba... it was very well done, but I have never done garba since school,"[12] he said.

International Laws to Regulate AI.

The speed at which artificial intelligence has advanced in recent years has prompted concerns about how ready governments and regulatory bodies are to protect the rights and welfare of their populations. Leaders in the industry have also voiced worry about how AI may eventually alter human lives. Applications of AI might have a significant impact on a variety of industries, including education and health. Furthermore, governments wish to participate in the trillion-dollar AI sector, which is not a creation of government laboratories as the internet was.

In April 2021, the European Commission released the first draft of regulations pertaining to AI in the EU. Brussels felt the need to reexamine the first proposal, nevertheless, given the availability of OpenAI's ChatGPT in 2022 and other technical advancements. In order to maintain human control over AI, the three arms of the Union reached an agreement about the framework of the bloc's AI legislation for the near future following three days of heated discussions.

After three years of proposed (and disabled) measures on the topic, Brazil now has a draft AI law. The paper carefully describes the rights of users engaging with AI systems and offers rules for classifying various forms of AI depending on the risk they represent to society. It was issued late last year as part of a 900-page Senate committee study on AI. Because of the law's emphasis on users' rights, AI suppliers are required to tell consumers about their products. Consumers have a right to be aware that the AI they are engaging with is but also the right to know how an AI

[11] *Ibid*
[12] *ibid*

 ISSN: 2582-6433

arrived at a certain conclusion or suggestion. Users have the option to challenge AI judgments or request human involvement, especially in cases where the AI decision is expected to have a substantial effect on the user, as in the case of self-driving vehicle, employment, credit evaluation, or biometric identity systems.

Though creators of high-risk goods are subject to an even higher threshold of culpability, all AI developers are accountable for harm produced by their AI systems.

China is looking for public feedback on a draft legislation it released about generative AI. China's proposal, however, states that generative AI must adhere to "Socialist Core Values," unlike most other nations. According to a translation of the draft legislation by Stanford University's Digi China Project, in its current version, developers "bear responsibility" for the content made by their AI. There are other limitations on where training data may be obtained; developers risk legal repercussions if their training material violates the intellectual property rights of third parties. Additionally, the rule mandates that AI services be created with the sole purpose of producing "true and accurate" material.

However, Italy temporarily outlawed ChatGPT due to worries about the manner and volume in which the chatbot was gathering user data. Israel and Japan have chosen a "soft law" approach to AI regulation, meaning that there are no strict laws dictating how AI may or cannot be employed in either nation. Instead, claiming a want to avoid restricting innovation, both nations have chosen to wait and observe how AI evolves.

Indian Legal Framework For Regulation Of AI

According to Hindustan Times, India's Ai market is likely to see a 20% rise in the next few years. Former CJI SA Bobde has also spoken about increasing and adapting AI in India legal system which may actually help clear a lot of case backlog. Gone will be the days when it would take 20 years to dispose of a criminal case or get a divorce.

At this point In India, there are no specific provisions that deal with AI, but the government is expressing concerns regarding the non-availability of these laws. Though Indian government has also set up a MeiTY (The Ministry of Electronics and Information Technology) in India. MeiTY is the regulatory body of AI in India. It has the responsibility development, implementation, and

 ISSN: 2582-6433

management of AI laws and guidelines in India. There is certain provision mentioned under Intellectual property law and several provision as Section 43A and 72A of information technology act 2000 which implies that if anyone commits crime by using AI, then he will be liable under IT act, criminal laws, and other cyber law. Information technology rules 2021 obligates the social media platforms to exercise greater diligence regarding content on their platforms.

Information Technology Act, 2000:

The primary piece of law guiding digital governance and electronic transactions is the Information Technology Act, 2000 (IT Act). Even though the Act doesn't specifically address AI, actions involving AI are covered by several of its sections. Compensation may be granted under Section 43A of the IT Act in the event that careless treatment of sensitive personal data results in a data privacy violation. This clause is especially pertinent when it comes to AI systems that handle user data. Section 73A of this legislation is an additional provision.

Personal Data Protection Bill, 2019:

The goal of the Personal Data Protection Bill, 2019 (PDP Bill), which is presently being considered, is to create a thorough framework for safeguarding personal data. The law adds principles and requirements, such as responsibility, consent, purpose limitation, and data localization, for enterprises processing personal data. It also suggests setting up a Data Protection Authority to supervise and implement the bill's requirements. Provisions concerning automated decision-making and profiling are included in the PDP Bill. When processing personal data using AI algorithms that significantly affect an individual's rights and interests, it requires the subject to give their explicit consent.

Indian Copyright Act, 1957:

Original literary, artistic, musical, and dramatic works are protected under the Indian Copyright Act, 1957, which grants artists exclusive rights and forbids unapproved use or duplication. "The rise of AI-generated content has prompted discussions regarding copyright ownership and infringement liability. Case Law: In the case of Gramophone Company of India Ltd. v. Super Cassettes Industries Ltd. (2011)[13], the Delhi High Court determined that AI-generated music produced by a computer program lacks human creativity and, therefore, is ineligible for copyright

[13] Gramophone Company of India Ltd. v. Super Cassettes Industries Ltd. (2011) 44, SCC 541 (India).

 ISSN: 2582-6433

protection. This case clarifies the copyrightability of AI-generated content in India."

AIRAWAT:

Niti Ayog, the Indian Planning Commission, recently introduced the AI Research, Analytics, and Knowledge Assimilation Platform, or AIRAWAT. It takes into account all of India's AI needs.

Conclusion

The methods AI raises serious privacy concerns, including the use of facial recognition software for surveillance, potential character theft from data breaches, biased profiling and discrimination, a lack of informed consent, and the secondary use of data without user knowledge. Notable challenges also include privacy concerns in healthcare and a lack of accountability and transparency in automated decision-making. The malicious use of personal data adds to the difficulty of these issues. To maintain a balance between advancing innovation and safeguarding fundamental privacy rights in the era of artificial intelligence, strong regulations, transparent AI frameworks, and customer empowerment are essential components of privacy security.