ARTIFICIAL INTELLIGENCE AND LEGAL LIABILITY

Saurabh Margonwar*

ABSTRACT

This legal research explores the intersection of artificial intelligence and legal liability focusing on the challenges and opportunities posed by AI systems in the context of existing legal framework. With AI systems increasingly involved in the decision-making process their potential to infringe on fundamental human rights and violate data privacy regulations has become a legal critical concern. The study analyses the adequacy of the current legal framework in addressing this issue highlighting a gap in accountability and enforcement, by examining case law regulatory approaches and ethical considerations. This paper evaluates the liability of AI when it violates human rights and privacy by analyzing case studies and jurisprudence. This research aims to provide actionable insight for policymakers, legal practitioners and technologies to ensure that AI innovation aligns with the principle of justice and accountability.

Keywords: Artificial Intelligence, Legal Liability, Human Rights, Data Privacy, Accountability.

INTRODUCTION

Artificial Intelligence (AI) has revolutionized the way industries function, offering unprecedented advancements in automation, decision-making, and problem-solving. From healthcare and autonomous vehicles to finance and education, AI technologies are becoming indispensable. However, their widespread deployment brings forth complex legal questions, particularly concerning accountability and liability when AI systems cause harm or fail to function as intended.

*LLB, SECOND YEAR, SHANKARRAO CHAVAN LAW COLLEGE.

Legal liability in the context of AI involves addressing questions such as: Who is responsible when an AI system malfunctions or causes harm? Should AI systems themselves bear some form of liability, or does the responsibility lie solely with their developers, users, or manufacturers? Who is liable when artificial intelligence violates fundamental human rights? Can we trust AI for data protection? These questions require a nuanced understanding of both existing legal principles and the challenges posed by AI's unique characteristics. This paper explores the legal frameworks, challenges, and potential solutions related to AI and liability.

According to Tim Cook "what all of us have to do is to make sure we are using AI in a way that is for the benefit of the humanity, not the determinant of humanity."

OBJECTIVE OF THE STUDY

The objective of this research is as follows-

1. To understand the wider concept of Artificial Intelligence and legal liability.
2. To analyze how AI violates fundamental human rights and data privacy.
3. Aims to provide actionable insight for policymakers, and legal practitioners.

RESEARCH QUESTION

1. To what extent can artificial intelligence be held legally accountable for violations of human rights and data privacy?
2. How should existing legal frameworks adapt to address these emerging challenges?

HYPOTHESIS

The research will bring to light the rights of people who are being infringed and will talk about whose liability it should be and how data privacy is infringed by AI. When harm is caused by autonomous AI systems, assigning legal liability will depend on the level of human oversight and the transparency of the AI's decision-making process.

I. WHAT IS ARTIFICIAL INTELLIGENCE AND HOW IT WORKS

Al is the intelligence that the machine demonstrates. It is an endeavour to replicate or simulate human intelligence. Al is the fusion of science, mathematics and computer science that uses complex algorithms and mathematical models to build intelligence. However, a common definition acceptable across the community does not seem to exist.

Nevertheless, keeping in view, its journey from being a mere academic discipline since its birth, to being the most disruptive breakthrough during the last five years with diverse approaches to research.

"Al is the science and engineering of making intelligent machines."

-John McCarthy (1956), father of AI

How does AI work?

In order to create AI, you need to: define the problem, determine the outcomes, organize the data set, choose the appropriate technology, and then test solutions. If the intended solution does not work, you can continue experimenting to reach the desired outcome.

- Input

  Data is first collected from various sources in the form of text, audio, videos, and more. It is sorted into categories, such as those that can be read by the algorithms and those that cannot. You would then create the protocol and criteria for which data will be processed and used for specific outcomes.

- Processing

  Once data is gathered and inputted, the next step is to allow AI to decide what to do with the data. The AI sorts and deciphers the data using patterns it has been programmed to learn until it recognizes similar patterns in the data that are being filtered into the system.

- Outcomes

  After the processing step, the AI can use those complex patterns to predict outcomes in customer behavior and market trends. In this step, the AI is programmed to decide whether specific data is a “pass” or “fail”—in other words, does it match previous patterns? That determines outcomes that can be used to make decisions.

- Adjustments

  When data sets are considered a “fail”, AI learns from that mistake, and the process is repeated again under different conditions. It may be that the algorithm’s rules must be

adjusted to suit the data set in question or that the algorithm needs slight alteration. In this step, you might return to the outcomes step to better align with the current data set's conditions.

- Assessments

The final step for AI to complete an assigned task is assessment. Here, the AI technology synthesizes insights gained from the data set to make predictions based on the outcomes and adjustments. Feedback generated from the adjustments can be incorporated into the algorithm before moving forward.

II. AI AND HUMAN RIGHTS

As we are at the cusp of technological change, history shifts its pace when touched with scientific vision. Artificial Intelligence (AI) is one such technical field that is transforming human society into one of robots and machines. AI includes machine learning, natural language processing, big data analytics, algorithms, and much more. However, as human intelligence is marked by intrinsic bias in decision-making, such characteristics can also be found in AI products that work with human-created intelligence. These phenomena of bias and discrimination – rooted in a cluster of technologies and embedded in social systems – are a threat to universal human rights. Indeed, AI disproportionally affects the human rights of vulnerable individuals and groups by facilitating discrimination, thus creating a new form of oppression rooted in technology.

But the question before us today — what the limits should be on artificial intelligence and emerging technologies — is one of the most pressing faced by society, governments and the private sector. We have all seen and followed over recent months the remarkable developments in generative AI, with ChatGPT and other programs now readily accessible to the broader public.

We know that AI has the potential to be enormously beneficial to humanity. It could improve strategic foresight and forecasting, democratize access to knowledge, turbocharge scientific progress, and increase capacity for processing vast amounts of information. But in order to harness this potential, we need to ensure that the benefits outweigh the risks, and we need limits.

- AI and its discrimination

AI algorithms and face-recognition systems have repeatedly failed to ensure a basic standard of equality, particularly by showing discriminatory tendencies towards Black people. In 2015, Google Photos, which is considered an advanced recognition software, categorized a photo of two Black people as a picture of gorillas. When keywords such as 'Black girls' were inputted into the Google search bar, the algorithm showed sexually explicit material in response. Researchers have also found that an algorithm that identifies which patients need additional medical care undervalued the medical needs of Black patients.

Facial recognition technology is now being adopted in the criminal justice systems of different states – including Hong Kong, China, Denmark and India – to identify suspects for predictive policing. Sceptics have pointed out that instead of mitigating and controlling police work, such algorithms instead enhance pre-existing discriminatory law enforcement practices. The unevaluated bias of these tools has put Black people at a bigger risk of being perceived as high-risk offenders, thus further entrenching racist tendencies in the justice and prison systems. Such racial discrimination inherited in AI disgraces its transformative implementation into society and violates equal treatment and the right to protection.

- AI brings unemployment

Artificial intelligence (AI) is rapidly transforming various sectors, leading to concerns about its potential impact on employment. While AI offers numerous benefits, it also poses a significant threat of job displacement.

One of the primary concerns is AI's ability to automate tasks previously performed by humans. AI-powered systems can now analyze vast amounts of data, identify patterns, and make decisions with increasing accuracy and speed. This capability has the potential to replace workers in a wide range of industries, from manufacturing and transportation to customer service and even certain creative fields. For example, self-driving cars could render millions of truck drivers redundant, while AI-powered chatbots could replace human customer service representatives.

Moreover, AI is not limited to automating routine tasks. It is also capable of performing complex cognitive functions, such as decision-making and problem-solving. This could lead to the displacement of highly skilled workers in fields like finance, law, and medicine. For

instance, AI-powered diagnostic tools could potentially replace radiologists, while AI-driven investment algorithms could outperform human fund managers.

The impact of AI on employment is likely to be uneven, disproportionately affecting low-skilled and repetitive jobs. Workers in these roles may lack the skills or resources to transition to new employment opportunities, exacerbating existing inequalities. Furthermore, the rise of AI could lead to increased income inequality, as the benefits of automation are primarily reaped by the owners of capital, while the costs are borne by workers who lose their jobs.

Adidas has moved towards 'robot-only' factories to improve efficiency. Thus, business growth no longer relies on a human workforce; in fact, human labor may negatively affect productivity. Until now, technology has had a more detrimental effect on low and middle-skilled workers, with decreasing employment opportunities and falling wages, leading to the emergence of job polarization. However, as technology continues to advance, many jobs that we would today consider protected from automation will eventually be replaced by AI. For example, AI-based virtual assistant software such as Siri, Cortana, Alexa and Google, have steadily replaced personal assistants, foreign language translators, and other services that were previously reliant on human interaction.

- AI and freedom of expression

Artificial intelligence (AI) has the potential to both enhance and restrict freedom of expression. On one hand, AI-powered tools can be used to censor content, monitor online activity, and spread disinformation. This can lead to the suppression of dissenting voices, the chilling of free speech, and the manipulation of public opinion.

On the other hand, AI can also be used to promote freedom of expression. AI-powered platforms can be used to identify and counter online harassment, hate speech, and other forms of harmful content. Additionally, AI can be used to personalize content recommendations, ensuring that individuals are exposed to a diversity of viewpoints.

The impact of AI on freedom of expression will depend on how it is developed and deployed. It is important to ensure that AI systems are designed and used in a way that respects human rights and promotes open dialogue. This can be achieved by implementing ethical guidelines, promoting transparency, and ensuring that AI systems are subject to human oversight.

- Controlling populations and movement

Freedom of movement derives itself from many international declarations and has been recognized as a fundamental individual right by many countries. AI's ability to limit this right is specifically related to its usage for surveillance purposes. A report from the Carnegie Endowment for International Peace pointed out that at least 75 of 176 countries globally are actively using AI for security purposes, such as border management. There have been concerns regarding the disparate impact of surveillance on populations that are already discriminated by police – such as Blacks, refugees and irregular migrants – as predictive policing tools end up factoring in "dirty data" reflecting conscious and implicit bias. The Guardian reported that to keep a check on illegal immigration, dozens of towers equipped with feature laser-enhanced cameras were installed at the US-Mexico border in Arizona. In addition to this, the US government deployed a facial recognition system to record images of people inside vehicles entering and leaving the country.

Technological shifts have also impacted the military and humanitarian sectors. The increasing use of armed drones in warfare – in particular by the US in Pakistan and Afghanistan – has been repeatedly denounced as a violation of International Humanitarian Law in a 2010 UN report. An investigation by The Intercept of US military operations against the Taliban and al Qaeda in the Hindu Kush revealed that nearly nine out of ten people who died in drone strikes were not the intended targets. The rapid development of autonomous technology and AI has also resulted in fully autonomous weapons such as "killer robots", which raise a host of moral, legal, and security concerns. The lack of ethical judgment of such machines has raised concerns about the reliability and error in judgment of these weapons, which might result in accidental deaths and the rapid escalation of conflicts. Indeed, Zachary Kallenborn's article highlights the incapability of these weapons to discriminate between combatants and non-combatants. The rapid increase in dependency on AI to enforce social control during the present pandemic has also raised many privacy concerns. Arogya-Setu dangerous mix of health data and digital surveillance, technologies are a potent threat to basic human rights and can be used as tools of exploitation and oppression. In fact, if the use of AI continues to remain widely unregulated, the human rights of vulnerable groups will undoubtedly suffer.

III. DATA PRIVACY CONCERN

In the digital era, personal data has become an incredibly valuable commodity. The vast amount of data generated online daily has enabled businesses, governments and organizations to gain new insights and make better decisions. In the context of AI, privacy is essential to ensure that the AI system is not used to manipulate individual or discriminate against them based on their personal data. It is a fundamental human right that is necessary for personal autonomy, protection and fairness. AI systems that rely on personal data to make decisions must be transparent and accountable to ensure that they are not making unfair or biased decisions.

- The use of AI in surveillance

One of the most controversial uses of AI technology is in the area of surveillance. AI-based surveillance systems have the potential to revolutionise law enforcement and security, but they also pose significant risks to privacy and civil liberties.

AI-based surveillance systems use algorithms to analyze vast amounts of data from a range of sources, including cameras, social media, and other online sources. This allows law enforcement and security agencies to monitor individuals and predict criminal activity before it occurs.

While the use of AI-based surveillance systems may seem like a valuable tool in the fight against crime and terrorism, it raises concerns about privacy and civil liberties. Critics argue that these systems can be used to monitor and control individuals, potentially losing freedom and civil liberties.

- Data collection and its use by AI technology

One of the most significant impacts of AI technology is the way it collects and uses data. AI systems are designed to learn and improve through the analysis of vast amounts of data. As a result, the amount of personal data collected by AI systems continues to grow, raising concerns about privacy and data protection. We only have to look at the various generative AI tools, such as ChatGPT, Stable Diffusion or any of the other tools currently being developed, to see how our data (articles, images, videos, etc.) are being used, often without our consent.

More importantly, the use of personal data by AI systems is not always transparent. The algorithms used in AI systems can be complex, and it can be difficult for individuals to

understand how their data is being used to make decisions that affect them. Lack of transparency can lead to distrust of AI systems and a feeling of unease.

- Biased and discrimination

Another challenge posed by AI technology is the potential for bias and discrimination. AI systems are only as unbiased as the data they are trained on; if that data is biased, the resulting system will be too. This can lead to discriminatory decisions that affect individuals based on factors such as race, gender, or socioeconomic status. It is essential to ensure that AI systems are trained on diverse data and regularly audited to prevent bias. To start with, it is important to note that many AI systems rely on data to make decisions. This data can come from a variety of sources, such as online activity, social media posts, and public records. While this data may seem innocuous at first, it can reveal a lot about a person's life, including their race, gender, religion, and political beliefs. As a result, if an AI system is biased or discriminatory, it can use this data to perpetuate these biases, leading to unfair or even harmful outcomes for individuals.

For example, imagine an AI system used by a hiring company to screen job applications. If the system is biased against women or people of colour, it may use data about a candidate's gender or race to unfairly exclude them from consideration. This harms the individual applicant and perpetuates systemic inequalities in the workforce.

IV. NEGLIGENCE AND STRICT LIABILITY

Negligence

Under negligence, a plaintiff must prove that the defendant owed them a duty of care, breached that duty, and that the breach caused harm. In the context of AI, negligence could arise from various situations:

a) Defective AI design: If an AI system is designed with flaws or vulnerabilities that could lead to harm, the developer or manufacturer could be held liable for negligence.
b) Inadequate training or testing: If an AI system is not properly trained or tested before deployment, and this leads to harm, the developer or user could be held liable.
c) Failure to monitor or maintain AI systems: If an AI system is not properly monitored or maintained after deployment, and this leads to harm, the user could be held liable.

d) Misuse of AI: If an AI system is used for purposes it was not intended for, or in a way that could reasonably be expected to cause harm, the user could be held liable.

Strict Liability

Strict liability holds a party responsible for harm caused by their actions, regardless of fault. This doctrine is often applied in cases involving ultrahazardous activities or defective products. In the context of AI, strict liability could be applied in the following situations:

a) Defective AI products: If an AI system is considered a product, and it is found to be defective, the manufacturer could be held strictly liable for any harm caused by the defect.
b) Ultrahazardous AI applications: If an AI system is used in an ultrahazardous activity, such as autonomous vehicles or weapons systems, the developer or user could be held strictly liable for any harm caused.

V. REGULATORY RESPONSE

India

India formally stepped into the Al arena in June 2018, when the apex think-tank of the Government of India, the National Institution for Transforming India (NIT Aayog) published the discussion paper on Al strategy titled 'National Strategy on Artificial Intelligence:
#AlforAll'. The Indian strategy focuses on economic growth and leveraging Al to enhance social inclusion. The strategy emphasises research to address issues of concern related to Al, i.e., ethics, bias and privacy issues. Five sectors have been chosen as key to the development of Al for economic growth. These are agriculture, healthcare, education, smart cities & infrastructure and smart transportation & smart mobility.
Funding by the government amounts to & 7000 Crores (USD 949
Million). In 2019, the Ministry of Electronics and Information Technology (MeitY) allocated 7,400 Crores for a national Al program.
Meanwhile, NITI Aayog has also published approach documents on the Principles of Responsible Al' and their 'operationalisation'. India has predominantly focussed on leveraging the benefits of Al for society and economic growth. The site development and deployment of Al-based systems and regulatory mechanisms to address ethical and privacy concerns by its use are being discussed. The sustained Al summer continues and

as Al development progresses, there will be an inflection point wherein the development and use of lethal autonomous weapons and autonomy within a robust regulatory framework possibly in place by then, will decide the hegemony of a nation. However, no nation will be willing to wait for laws and regulations to be in place, before developing the potential that holds the key, both for the technological edge and national security.

Europe

For example, initiatives like the EU AI Act focus regulatory oversight on technical factors, such as the computing power used during training or fine-tuning an AI model. Similarly, the product liability structure for AI tends to emphasize unsafe product attributes while downplaying the human decision-maker role.

Other suggestions, such as strict liability or comparing sentient AI to wild animals or children, also shy away from addressing the human processes involved in AI development. This focus on technology can allow AI creators to separate themselves from the potential consequences their systems might cause.

Asia

Several Asian countries have made considerable progress in developing AI-related data protection laws. China focuses on tight control, emphasizing national security and social stability. Its Personal Information Protection Law (PIPL) imposes strict rules on collecting and using personal data in AI applications and restricts algorithms in areas like online content censorship.

With its updated Personal Information Protection Act (APPI), Japan aims to protect citizens' data in an AI-driven world. At the same time, South Korea takes a balanced approach, promoting innovation while safeguarding fundamental rights, with less restrictive regulations than China.

Mexico

Like other countries in Latin America, Mexico is in the initial stages of developing regulatory frameworks for AI. While Mexico is keen on aligning with global AI trends, it faces challenges, such as the need to integrate existing trade and data protection laws into its regulatory efforts. Currently, the country lacks a comprehensive legal framework

specifically for artificial intelligence. In 2023, Mexico pushed forward by setting up the National AI Alliance. Supported by various experts and a Mexican senator, this initiative aims to strengthen the AI ecosystem and lay the foundation for future AI legislation. While Congress has recognized the need for AI regulation, no formal laws have been passed yet.

United States of America

On 11 February 2019, then-President Donald Trump launched the American Al initiative, the Nation's Strategy for promoting Amerite leadership in Al. It prioritised the need to invest in R&D and Insane safe development, testing and deployment of Al technologies. The White House also stressed developing an Al-ready workforce and collaboration with foreign partners while promoting U.S. leadership
in Al.

As far as funding is concerned, it is unclear as regards the Government's investment in Al. The Pentagon spent approximately US$ 7.4 billion on Al in its 2017 budget, as per an article by Tim Dutton, an Al policy researcher based in Canada. Significantly, the growth in R&D for Al has been phenomenal since 2015, and it may likely be due to military and defence agency Al's efforts.

The US government released its first annual report in February 2020 followed by guidelines in November 2020 for federal agencies to regulate Al applications in the private sector, to include principles governing Al innovation and growth and build public trust and confidence in Al technologies. The National Defence Authorisation Act (NDAA) for Fiscal Year 2021 is directed to coordinate AI research and policy across the federal government.

VI. CASE STUDY

1. Google's Location Tracking

Due to privacy concerns, Google's location-tracking practices have come under intense scrutiny in recent years. The company tracks the location of its users, even when they have not given explicit permission for their location to be shared. This revelation came to light in 2018 when an Associated Press investigation found that Google services continued to store location data, even when users turned off location tracking. This was a clear breach of user trust and privacy, and Google faced significant backlash from users and privacy advocates.

2. The Use of AI in Law Enforcement

   One example of the use of AI in law enforcement is the deployment of predictive policing software. This software uses data analysis and machine learning algorithms to predict where crimes are most likely to occur and who is most likely to commit them. While this technology may sound promising, it has come under scrutiny for perpetuating biases and reinforcing existing prejudices. For example, some predictive policing systems have been found to unfairly target minority communities, leading to allegations of racial profiling and discrimination.

3. Sushil Kumar Sharma Vs. Union Of India

   Supreme Court of India agreed to appeal for the necessity of the complete legal law for the Artificial Intelligence.

WAY FORWARD

Developing Comprehensive AI Regulations: Governments should establish clear, harmonized regulations that define liability standards for AI systems.

Promoting Transparency: Mandatory documentation of AI development processes and decision-making algorithms can aid in liability assessments.

Encouraging Industry Self-Regulation: Industry standards and best practices should complement legislative efforts to ensure responsible AI development.

Investing in Legal Education: Training legal professionals to understand AI technologies will enhance their ability to navigate complex liability cases.

Public Engagement: Engaging stakeholders, including the public, in discussions about AI liability can foster trust and legitimacy

REFERENCES

1. Law governing AI in India by Divya Saraswat. (Link)
2. Research paper of The Amikusqriae
3. Artificial intelligence liability- blog by Ryan Long
4. Blog- Beginning of Artificial Intelligence and end of human rights
5. Privacy in the age of AI by Dr.Mark
6. Artificial Intelligence and National Security by Vijay Khare and Amit Sinha