LEGALFOXES LAW TIMES

Harmonizing Artificial Intelligence and Privacy: A Comparative Analysis with Special Focus on India

By Mahima Nayak* and Sathyajith M S**

ABSTRACT

This paper attempts to briefly explain the scope and meaning of Artificial Intelligence (AI) and how AI-based models are created and work. The current debate about AI models mostly revolves around the harmful effects of the advent of AI on one side vis-a-vis the humongous benefits and convenience that AI offers on the other. Within the legal fraternity, it revolves around the nature of the legal personality of AI. This essay presents the positive and negative aspects of AI models and the consequences that may arise if they are considered as a legal person or otherwise. It attempts to show a glimpse of the current scenario of AI regulations regarding privacy through a comparative analysis of legal framework in the USA, the EU, and Israel. It further intends to examine the development of the legal framework on privacy aspects relating to AI in India and explore the plausible regulations that India can adopt.

INTRODUCTION

Today, Artificial Intelligence (AI) has become an inseparable aspect of a country's development agenda. The same can be noticed when we realize that it is easier to identify the aspects in our daily lives and businesses which have not been impacted by AI.[1] It would not be an exaggeration to say that we can't imagine our society without AI.[2] This is because the AI machines can absorb, interpret, and make complex decisions which outpace the ability of humans to do similar

*Student, University Law College, Bangalore University.
**Student, University Law College, Bangalore University.

[1] Benard Marr, "What Is the Importance of Artificial Intelligence (AI)", *Bernard Marr & Co., available at*https://bernardmarr.com/default.asp?contentID=1829 (last visited on June 18, 2020).

[2] *Ibid.*

functions.[3] Hence, with the rapid development of AI in the 21st century, all countries are gearing up to be ahead of each other in its implementation and advancement. This development also requires an efficient, sustainable, and strong legal framework which governs different aspects of AI.

MEANING OF AI

AI, as the name itself suggests, is intelligence or ability which is artificial, and not human. It is a technique expressed by a machine or a non-human entity that has characteristics or abilities of a human, like problem-solving, decision making, and speech recognition *inter alia*. It trains computers into accomplishing complex tasks that usually require human intelligence. AI is typically defined as the "*science of making computers do things that require intelligence when done by humans*".[4] Hence, the goals of AI include learning, reasoning, and perception.[5]

While discussing AI, we also have to give cognizance to terms like Machine Learning and Neural Networks which are involved in developing the AI machines.

Machine Learning is an application or sub-field of AI where the machine learns by itself by utilizing the provided data without the interference of a human. Its primary task is to predict the future or do something it wasn't programmed to do. For example, Netflix suggesting its users watch a show or movie based on their previous viewing pattern. At its core, Machine Learning is a simple way of achieving AI.

The Neural Network is a computer system modeled after the human brain. In simple words, a neural network is a computer simulation of the way biological neurons work within a human brain.[6] It is aimed at solving complex tasks by exposing a system to a large amount of data. The

[3] What is Artificial Intelligence?*Net app*, *available at*https://www.netapp.com/us/info/what-is-artificial-intelligence-ai.aspx (last visited on June 18, 2020).

[4] Stefan van Duin & Naser Bakhshi, "Part 1: Artificial Intelligence Defined", *Delloite*, March 2017, *available at* https://www2.deloitte.com/fi/fi/pages/technology/articles/part1-artificial-intelligence-defined.html (last visited on June 18, 2020).

[5] Jake Frankenfield, "Artificial Intelligence", *Investopedia*, March 13 2020, *available at* https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp (last visited on June 18, 2020).

[6] Tanmoy Ray, "Demystifying Neural Networks, Deep Learning, Machine Learning, and Artificial Intelligence", *Stoodnt*, March 29, 2018, *available at* https://www.stoodnt.com/blog/ann-neural-networks-deep-learning-machine-learning-artificial-intelligence-differences/ (last visited on June 18, 2020).

system is then allowed to learn on its own how to make the best predictions. It solves problems using mathematical models like linear algebra, calculus (differentiation), etc. Thus, we can say that the neural network is the core and behind the output/result that we receive in facial recognition, music recommendations, targeted advertisement, cancer prediction. Hence, we can arrange it like this: Artificial Neural Networksor ANNs are types of Machine Learning models which in itself is subclassed as AI. AI is used interchangeably with Machine Learning and Deep Learning, and more often than not AI is used as a marketing term whereas Machine Learning is a more technical term.

LEGAL PERSONALITY OF AI

The legal framework has to evolve to cater to the technological changes and advancements. With advancement in technology, the vacuum to deal with novel legal issues arises due to the legislative void which exists. An efficient, precise, and effective legal framework prevents such complex legal disputes. It is seen that the lack of understanding and defining the legal personality of AI has led to various problems when it comes to determining the liability of a person. For example, in the case of *Jones v. W + M Automation, Inc.*[7], a court in New York state held that the defendant was not liable for the injury caused to a worker by a robotic gantry loading system, because the manufacturer had complied with the prescribed regulations.[8]

This emphasizes the need to establish a legal definition of AI and determine its legal personality. A 2016 report by the European Parliament's Committee on Legal Affairs[9] questions whether robots "should be regarded as natural persons, legal persons, animals or objects – or whether a new category should be created."

It is pertinent to note that a person is in general usage, a human being (i.e. a natural person), though by statute the term may include a firm, labour organizations, partnerships, associations,

[7] 818 N.Y.S.2d 396.

[8] Jeremy Elman & Abel Castilla, "Artificial Intelligence and the law", *Techcrunch*, January 28, 2017, *available at*https://techcrunch.com/2017/01/28/artificial-intelligence-and-the-law/(last visited on June 18, 2020).

[9] European Parliament, Committee on Legal Affairs, *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics*, 2015/2103(INL), PR\1095387EN.doc (May 31, 2016).

and corporations.[10] A person may be natural, or juristic. A juristic or a legal person is any subject matter other than a human being to which law attributes personality.[11] Therefore, it can be said that a legal person is an entity to which rights and duties can be attributed.[12]

In the context of AI, the lacuna in the legal framework is evident when the traditional legal principles may not be sufficient to deal with the problems arising out of AI. For example, since AI is considered to be lifeless, during the occurrence of default, who is to be held liable? The model or the producer or manufacturer of the model? In the context of law relating to contracts, since the legal personhood of AI is ambiguous, can any contract involving AI be held void or valid? Further, when the AI is capable of taking autonomous decisions, is it possible to hold the manufacturer liable for any unlawful act or omission? Of course, considering that AI is inanimate, it is to be assumed that we cannot hold the model to be liable but the manufacturer can be held liable.

Recently, Saudi Arabia accepted an AI-based robot, Sophia, as its citizen, thereby conferring a legal personality. This led to various deliberations on whether other countries should follow the suit and confer a legal personality that is equivalent to that of citizenship? Even if the law cannot confer citizenship, can rights and duties be ascribed to such AI-based robots is another aspect which requires analysis.

In the context of Sophia, if the robot is recognized as a natural person, then it is entitled to rights, responsibilities, duties, can vote, pay tax, defend the country. If recognized as an artificial person like a company, then it will have rights and duties but no other obligations and privileges conferred to natural persons.

With such ambiguities, there is a need to recognize a new category of persons in the law. This has been emphasized in the report of the European Committee wherein it has suggested the creation of a special legal status called "Electronic Person" which can be ascribed to AI models or humanoid AI models. This should have its qualities wherein liabilities can be determined for

[10] Sumeet Malik, *Concise Law Dictionary* (Eastern Book Company, Lucknow, 2016).

[11] *Ibid.*

[12] Vinita Kumari, "Changing the dimension of person under different law" 1 *Indian Legal Solution Journal of Criminal and Constitutional Law* (2019).

any acts or omissions of the AI-based robots while limiting conferment of rights such as that of citizenship.[13]

LEGAL REGULATION OF AI

While the determination of legal personality is a jurisprudential aspect of the law, with the rapid development of AI, it is pertinent for every country to regulate AI and its models to prevent misconduct and threat to society. While the regulation of AI is still in its infancy, countries are framing policies which emphasize on various legal issues, including data protection and privacy, transparency, human oversight, public administration and services, Lethal Autonomous Weapons Systems (LAWS)[14] and autonomous vehicles. The development of regulation has been significant in the field of autonomous vehicles primarily. However, since the scope of analysis of this paper is on privacy aspects relating to AI specifically, areas relating to autonomous vehicles and LAWS is beyond its scope.

COMPARATIVE ANALYSIS OF PRIVACY AND AI IN DIFFERENT JURISDICTIONS

The Privacy of an individual is considered one of the basic human rights that all individuals enjoy. The right to be let alone or right to privacy has been recognized in various jurisdictions across several democratic nations, and international law. The Universal Declaration of Human Rights (UDHR) clearly states that "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".*[15]

With Artificial Intelligence being the current talking point, it is pertinent to give cognizance to the advancement of AI along with the data collected for the efficient functioning of the same system. As AI-based models mainly work on the inputs or the data provided by the users, the protection of personal data is the need of the hour.

---

[13] *Supra* note 10.

[14]Congressional Research Service, "Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems" (December 19, 2019).

[15] The Universal Declaration of Human Rights, 1948, art. 12.

As far as reconciling data protection and privacy vis-a-vis the advancement of AI is concerned, it can be said that it is a herculean task if not anything less. This conundrum arises because a rigid data protection regime may weaken the advancement of AI. The Advancement of AI largely depends on the historical data inputs. At the same time, it is hard to forgo the concerns of privacy which is as essential as the convenience that AI brings to the table. Today, machine recognition of faces has progressed rapidly from fuzzy images of cats to rapid recognition of individual humans. For instance, facial recognition used in mobile phones or surveillance cameras collectsindividuals' personal data which if not regulated strictly might be misused by the authorities collecting the data for their benefit. Facial recognition systems are also being deployed in and around the cities of various countries that lack the data protection legal framework, thereby increasing the concerns regarding privacy.

Additionally, there are also ethical concerns about the methods adopted by AI in collecting data of individuals. When there are a lawful method and basis prescribed for collecting the data of individuals, there can be no guarantee that the AI model will follow these guidelines when they are given the flexibility to collect data. For example, if the AI has been programmed to collect data relating to the health of individuals, we cannot guarantee that they would adhere to the guidelines prescribed. With such complex problems, it has become a challenge for legislators across the globe to come up with novel techniques and methods to provide comprehensive solutions by balancing privacy concerns with the advancement of AI. However, the work is in progress and many countries such as the USA, Israel, and the EU have made attempts to address the problems through guidelines, regulations, laws *inter alia*. The comparative analysis regarding regulations that exist in the USA, European Union, and Israel concerning aspects relating to data protection and privacy of AI-based models which may be relevant for India to adopt, has been provided below.

Artificial Intelligence and Privacy in the USA:

As far as the USA is concerned, there is no umbrella legislation regarding privacy. The regulation is industry and sector-specific. Data protection and privacy laws in the USA are not horizontally applicable, rather have vertical applicability. Therefore, unlike the European Union

(EU), the USA has no data protection law at the federal level. However, some states like California have legislation which is similar to the GDPR.[16]

It is pertinent to make note of the fact that privacy, data protection, and data security concerns are dealt with by the US Federal Trade Commission (FTC) which is empowered to look into "deceptive practices" by the companies. It has been said that this includes the company doing any act against its published privacy commitments. Apart from this, privacy concerns have been incorporated in other sector-specific legislations like Driver's Privacy Protection Act, 1994 which regulates the usage of personal information collected by the motor vehicle authorities at the state level.[17] Nevertheless, with AI taking the center-stage in our society, it is evident that the FTC is not empowered to regulate privacy concerns when it comes to AI. This emphasizes the need to incorporate data protection and privacy concerns in a specialized AI legislation.

The need to incorporate the protection of privacy concerns and the handling of data has been recognized in the USA. The Report of the Committeeon Artificial Intelligence (2016)[18] delves into the aspects relating to privacy vis-a-vis the development of AI and provides noteworthy suggestions. There are several bills such as the Future of AI Act, 2017, Innovative and Ethical Data Use Act of 2019, Consumer Online Privacy Rights Act *inter alia*. The House of Representatives also passed a resolution in 2019 regarding the development of guidelines for the ethical development of artificial intelligence. Among other things, it suggests the development of AI intending to guarantee information privacy and protection of one's data.[19]

The Innovative and Ethical Data Use Act of 2019 highlights the major concerns relating to privacy and empowers the US FTC to make rules and regulations to have a comprehensive privacy program. However, this does not extend to AI-based machines and programsper se. It broadly extends to the companies and corporations which have been defined under "Covered

[16] Andy Green, "Complete Guide to Privacy Laws in the US", *Varonis*, March 29, 2020, *available at*https://www.varonis.com/blog/us-privacy-laws/ (last visited on June 18, 2020).

[17] Steven Chabinsky & Fr. Paul Pittman, "USA:Data Protection 2019", *ICLG.com*, July 3, 2020, *available at*https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (last visited on June 18, 2020).

[18] The White House Office of Science and Technology Policy, "Summary of the 2018 White House Summit on Artificial Intelligence for American Industry" (May 10, 2018).

[19] H.Res.153 -Supporting the development of guidelines for ethical development of artificial intelligence, 2019.

Entities". Similarly, the Consumer Online Privacy Act also deals with placing requirements on entities that process or transfer a consumer's data. If a company uses AI to process and transfer data, the liability for any mistake is unclear. While the AI can be programmed by incorporating the guidelines provided in the bill, it is unclear whether the company using the AI can be held vicariously liable.

The ambiguity regarding the above-mentioned scenario has been potentially addressed by the Algorithmic Accountability Act of 2019 which provides for empowering the FTC to 'conduct automated decision system impact assessments and data protection impact assessments'.[20] This Act has now been referred to the Committee on Commerce, Science, and Transportation. The Act clearly defines the term 'Automated Decision System' which includes AI. The Act broadly sets out the guidelines to conduct assessments and promulgate regulations regarding the same within two years of the enactment coming into force. It directs the Data Protection Authority provided in the Act, to conduct data protection impact assessments of existing high-risk information systems. It also provides for the assessment of new high-risk assessment systems before its implementation. Therefore, it can be seen that with the prevailing ambiguity on the legal personality of AI, the lawmakers in the USA are exploring ways to overcome the issue by specialized legislation on data protection and privacy. While such legislations are laudable, it is to be kept in mind that imposing overburdening liabilities on the creators of AI may impede its development.

Artificial Intelligence and Privacy in the European Union:

AI capabilities are advancing rapidly and to harness AI's full potential, the legal concerns often raised regarding its collection and use of personal data, and unpredictability in its output requires to be confronted. Hence, the European Union (EU) has introduced the General Data Protection Regulation (GDPR) for the regulation of technologically collected data which took effect on May 25, 2018. It is applied directly to all EU Member States without any implementing legislation needed. Unlike the USA, the GDPR has broader, horizontal applicability in the EU.

The GDPR does not specifically refer to AI, but rather regulates the collection and use of personal data regardless of the technology used, as previously mentioned. Any processing of

[20] Algorithmic Accountability Act, 2019.

personal data through an algorithm falls within the scope of the GDPR.[21] As a consequence, any technology that is designed to process personal data, including AI, is fully encapsulated by the regime. Therefore, the collection of personal data by AI systems falls within the regulations of GDPR and all the EU member states must develop AI in compliance with the GDPR. However, it is pertinent to note that not all AI systems collect personal data. Some are built to collect non-personal, anonymous data too, but the line between personal and non-personal data has increasinglybecome obscure. This is mainly because of the lack of anonymization techniques.

Before collecting or processing any personal data, some very important and basic statutory provisions of the GDPR are to be fulfilled. Article 5 of the GDPR[22] lays down six principles which have to be fulfilled by the AI systems for processing of personal data. The personal data collected must be processed lawfully, fairly and there must be transparency. Only adequate and relevant data must be collected and for specified and legitimate purposes only. Appropriate security of the personal data must be ensured including adequate protection against loss, destruction, or damage of the personal data.

The collection and processing of data by AI systems have to be also on par with Article 6(1) of the GDPR[23] which lays down six provisions some of which include consent, the performance of a contract, compliance, legal obligation *inter alia.* Processing of data will be lawful only if atleast one of the six prerequisites are fulfilled.

One of the important aspects of AI is the automated decision-making. It is a process of deciding by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Article 22 of the GDPR[24]specifically regulates data involved in automated decision making by AI systems which include profiling[25] as well. Individuals have the right to not be subject to a decision based solely

[21]Centre for Information Policy Leadership, "Artificial Intelligence and Data Protection: How the GDPR Regulates AI" 4 (March, 2020).

[22] General Data Protection Regulation, 2018, art. 5.

[23]*Id.* at art. 6.

[24]*Id.* at art. 22.

[25]*Id.* at art. 4 (4).

on automated processing, including profiling. However, this is not applicable in all cases and has few exceptions. For example, when the individual has given explicit consent or when it is necessary for the performance of a contract.

The EU Commission has established a High-Level Expert Group (HLEG)[26] which comprises 52 experts to set out a framework for achieving a trustworthy AI. HLEG has laid down several principals that businesses should meet while designing AI systems. These principles are not limited to data privacy yet they overlap with the requirements of GDPR.

The GDPR extensively regulates AI and addresses many of the potential risks and challenges associated with the processing of personal data through algorithms. In case of implementation of new legislation, it must be on par with the GDPR to avoid duplicity.

Artificial Intelligence and Privacy in Israel:

Israel recently enacted Privacy Protection Regulations (Data Security), 5777-2017 according to the Privacy Protection Act, 5741-1981 to enforce the data protection requirements enumerated in the latter. Additionally, Human Dignity and Liberty, 5752-1992 establishes a constitutional right to privacy. There are other laws such as the Credit Data Law, 5776-2016, Biometric Identifiable Means and Information in Identifying Documentation and Database, 5770-2009 *inter alia*.[27] There can be no second thought over the fact that Israel has been one of the pioneers in legislating on privacy. Nevertheless, the advent of AI has opened up new concerns regarding privacy and data protection, and it is laudable that the law-makers have taken cognizance of the same. For instance, Chairman of the Science Committee Uri Maklev suggested the government review various aspects of AI such as privacy, legal liability, etc.[28]. The need to come up with specific legislation may also address other concerns such as that of online privacy for which there is no specific legislation.[29]

[26] EC, HLEG, *Ethics Guidelines for Trustworthy AI* (April 8, 2019).

[27] Ohad Elkeslassy, "Israel: Data Protection 2019", *ICLG.com,*and July 3, 2019, *available at*https://iclg.com/practice-areas/data-protection-laws-and-regulations/israel (last visited on June 18, 2020).

[28]Library of Congress, "Regulation of Artificial Intelligence: Middle East and North Africa" (November 6, 2019).

[29] DLA Piper, "Data Protection Laws of the World" (January 14 2020).

As is the case with other countries, balancing privacy concerns and data protection on one hand, and the development of AI on the other has been a challenge to the legislators. However, it has been noticed that Israel has found a way to balance both, keeping the desirability of the same aside. In the field of AI-based medical research, a national programthat requires the health records of Israelis accumulated during the last 30 years was announced.[30] The health records included clinical data and genetic data, which comes within the scope of 'sensitive personal data'.[31] This raised privacy concerns, and it was further alleged that the consent of individuals was not obtained to use their data for the aforesaid purpose.

To address privacy concerns, the government came up with two solutions i.e., de-identification and the option to 'opt-out' of this. De-identification assigns a particular code to an individual's data, ergo,non-revelation of the true identity. However, it has to be noted that this only makes it difficult to trace the true identity, and not make it impossible. As far as 'opting out' is concerned, it is based on the presumption that if an individual chooses to stay in, there is an implicit consent to use the individual's data for the program. Implied consent is recognized by law under the Privacy Protection Act, 5741-1982.[32] However, some commentators suggest that this concept of 'opt-out' amounts to ridiculing privacy since consent has to be taken in advance.[33] While the concerns raised may hold water, it is to be noted that Israel has been proactive and deserves credit in regulating AI in the manner it deems fit.

ARTIFICIAL INTELLIGENCE IN INDIA

A study by Canada's International Development Research Centre has shown that India is ahead of China and Israel in readiness of embracing AI.[34] According to *Crunchbase* data, there are 751

[30] Haim Ravia, "Challenges to AI medical research under Israeli law", *Lexology*, October 24 2018, *available at*https://www.lexology.com/library/detail.aspx?g=c2532d17-98e8-4b24-913a-0b1581ba8fca(last visited on June 18, 2020).

[31]*Supra* note 30.

[32] Protection of Privacy Law, 5741-1981, s. 3.

[33]*Supra* note 31.

[34]Hindol Sengupta, "Mission Artificial Intelligence", *Fortune India*, November 30, 2019, *available at* https://www.fortuneindia.com/polemicist/mission-artificial-intelligence/103838(last visited on June 18, 2020).

companies in India which majorly operate in the field of AI.[35] Some estimates suggest that AI will boost India's annual growth rate by 1.3% by 2035.[36] This roughly translates to $1 trillion of the Indian economy. In this context, with AI set to dominate the society, and the position that India occupies in the world provides the opportune moment for India to catapult itself as a leader in AI throughout the 21st century. However, for this, as the saying goes '*With great power comes greater responsibility'*, apart from focusing on AI education and research, a comprehensive and conducive legal framework is necessary to mitigate the negative impacts of AI without substantially hampering the advancement of AI.

The government has taken significant if not sufficient steps to catch up with the advancements. NITI Aayog, the government think-tank has come out with a discussion paper titled 'National Strategy for Artificial Intelligence'. Apart from this, to create a policy framework for AI, the Ministry of Electronics and Information Technology established four committees, of which one is 'Committee on Cybersecurity, Safety, Legal and Ethical issues'. In its draft report submitted to the government, the committee has dealt with privacy aspects relating to AI.

Data Protection Law:

India presently does not have an umbrella data protection law like the EU. Presently, under the Information Technology Act, 2000, there are some provisions that relate to data protection and privacy.[37] It is pertinent to note that privacy was recognized as a fundamental right only recently by the Hon'ble Supreme Court of India.[38] Around the same time, the Union Government constituted a committee to suggest a data protection framework.[39] The committee then submitted

[35] Crunchbase, "India Artificial Intelligence Companies", *available at*https://www.crunchbase.com/hub/india-artificial-intelligence-companies#section-overview(last visited on June 18, 2020).

[36] Nishant Malhotra & Saransh Roy, "National Artificial Intelligence Mission", *Invest India,* August 5, 2019, *available at* https://www.investindia.gov.in/team-india-blogs/national-artificial-intelligence-mission(last visited on June 18, 2020).

[37] Naqeeb Ahmed Kazia & Stephen Mathias, "Data protection and privacy in India", *Lexology*, https://www.lexology.com/library/detail.aspx?g=d1edde8f-71b9-49cb-b333-35fcae73402b(last visited on June 18, 2020).

[38]*K.S.Puttaswamy v. Union of India,* (2017) 10 SCC 1.

[39] Surabhi Agarwal, "Justice BN Srikrishna to head Committee for data protection framework", *Economic Times*, August 1, 2017, *available at* https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection-framework/articleshow/59866006.cms(last visited on June 18, 2020).

a draft Personal Data Protection Bill, which has been approved by the Prime Minister's Office and the Cabinet after watering down some provisions. This Bill runs along with the 2017 judgement by the apex court which declared Right to Privacy as a fundamental right, and the GDPR. It aims at protecting the data of individuals of India and regulates the entities that collect and have access to this data.

The draft bill identifies three categories of data: *Sensitive data* includes information on financials, health, sexual orientation, genetics, transgender status, caste, and religious belief. *Critical data* includes information that the government stipulates from time to time as extraordinarily important, such as military or national security data. The third is a *general category*, which is not defined but contains the remaining data.[40] The approved bill also provides for the establishment of a Data Protection Authority (DPA) to regulate and enforce data protection laws. Presently, this bill has been referred to a Joint Parliamentary Committee (JPC) for further examination and analysis.

AI and Privacy in India:

With a law on data protection still being a 'work in progress', India lacks a policy framework to address several privacy issues that are already arising due to the development of AI. The Data Protection Bill does not specifically protect privacy rights against automated decision making.[41] The discussion paper by NITI Aayog also suggests instituting a data privacy legal network, and sectoral regulations concerning privacy, security, and ethical aspects of AI.[42] The Report submitted by the Task Force on Artificial Intelligence also provides suggestions to tackle issues

[40] Vijay Govindarajan, Anup Srivastava, *et. al.*, "How India Plans to Protect Consumer Data", *Harvard Business Review*, December 18, 2019, *available at* https://hbr.org/2019/12/how-india-plans-to-protect-consumer-data (last visited on June 18, 2020).

[41] Amber Sinha & Elonnai Hickok, "The Srikrishna Committee Data Protection Bill and Artificial Intelligence in India", *The Centre for Internet Society India*, September 3, 2018, *available at*https://cis-india.org/internet-governance/blog/the-srikrishna-committee-data-protection-bill-and-artificial-intelligence-in-india(last visited on June 18, 2020).

[42] Divjyot Singh, Kunal Lohani, *et. al.*,"AI Machine Learning & Big Data 2020 India", *Global Legal Insights*, *available at* https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/india#chaptercontent6(last visited on June 18, 2020).

concerning privacy and data protection.[43] The draft report by the Committee on Cybersecurity, Safety, Legal and Ethical issues delves into privacy concerns and AI substantially.

The draft report recognizes the inherent risks of AI models concerning privacy breach and the unforeseen asymmetries that these models may produce in the long run.[44] It also suggests the use of methods such as 'anonymisation' or 'de-identification', whereby datasets are processed to remove data that relates tothe true identity of individuals. While taking note of the Bureau of Indian Standards (BIS) setting up a committee for standardization in AI, it further recommends the need to coordinate and collaborate at an international level where similar standards are being developed. In another section, the draft report calls upon the government to establish the necessary infrastructure for safety testing and certification of AI.

The draft report recommends setting up a robust anonymization infrastructure in order to make large sets of data available to the public for development. It also suggests the establishment of a National Resource Center for taking initiatives such as monitoring technological development, cybersecurity, sharing best practices *inter alia,* and function as a nodal agency to deal with other related issues such as safety, ethical and legal issues.

After having analyzed the privacy aspects regarding AI of the EU, the USA, and Israel, the authors recommend the following measures which the government may undertake:

- Enact the Personal Data Protection Bill at the earliest to provide a foundation for developing sector-specific privacy laws in the future.
- BIS to come up with privacy standards like encryption standards that AI-based systems should meet. Data Protection Authority should be empowered to examine whether the AI-based systems are meeting the required criterion and publish a 'privacy risk-assessment' report regularly.
- Develop anonymisation infrastructure for 'Sensitive personal data'; other data which may infringe the privacy of the individual, such as 'personal data', maybe de-identified. The

[43] Report of Task Force on Artificial Intelligence (March, 2018) *available at*https://dipp.gov.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf(last visited on June 18, 2020).

[44] Ministry of Electronics and Information Technology,"Draft report Committee on Cybersecurity, Safety, Legal and Ethical issues" (December 2019).

National Resource Center (as recommended in the Draft Report of Committee on Cybersecurity, Safety, Legal and Ethical issues) to take up the function which shall be monitored by the Data Protection Authority. However, in the long run, even 'personal data' should be anonymized.

- The Data Protection Authority should enforce regulations regarding the consequences of decisions taken by automated means. It may use the GDPR model to hold companies accountable and seek an explanation for the decisions taken by automated means.[45]
- Data Protection Authority should issue guidelines of AI chatbots. The General public should be informed if they are communicating with a chatbots or a human. This can be based on Bot Disclosure Law[46] passed by California in the USA.

CONCLUSION

A country's progress is determined by its advancement in technology and the level of growth in AI plays an essential role in determining the same. Since AI eases the heavy load of work and is efficient than manual labour, countries are implementing AI in every possible sector including health, military, agriculture, education, and many others, thereby resulting in the progression of the economy. It must be ensured that the data collected by these AI models are processed and stored in a secure server and it can be possible only when there are strict regulations for the same because privacy cannot be compromised.

For a country as dense as India which is taking measures to implement AI in its many sectors, data protection law is the need of the hour which must be implemented as early as possible for the companies to collect and process personal data with utmost precaution.This is necessary for individuals to trust the companies that are collecting their data. Only when there is a trustworthy AI, will there be cooperation and contribution from individuals for the advancement of AI. However, laws and regulations must be flexible to be amended as the technology advances and must not be too strict which might hinder the development of technologies, including AI.

[45] *Supra* note 42.

[46] Robert B, "How to Comply with California's Bot Disclosure Law", *Terms Feed*, October 4, 2019, *available at*https://www.termsfeed.com/blog/ca-bot-disclosure-law/(last visited on June 18, 2020).