International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

REGULATION OF ARTIFICIAL INTELLIGENCE IN INDIA: LEGAL PERSONHOOD AND LIABILITY

Priyanka Majumdar[1], Rupal Rautdesai[2], Bindu Ronald[3]*

[1,2,3] Symbiosis Law School, Pune, Symbiosis International (Deemed University), Pune India

[3]*Email: bronald@symlaw.ac.in

Abstract

The cutting-edge Artificial Intelligencetechnologies open a whole gamut of opportunities and threats raising ethical, legal and moral concerns.The increasing interaction of the Artificial Intelligence (AI) system with the human and natural environmentrequires us to be prepared to address any damage or legal injury resulting therefrom. The current regulatory framework at the national andinternational level is inadequate to address and govern thearray of ethical and legal issues that AI poses today or will pose in the near future.Currently, there is no legal framework governing AI in India. Based on jurisprudential and sociological constructs and theories, the paper analyseswhether conferring of legal personhood upon such AI entities under the Indian law may be appropriate to address liability issues.The paper discusses the existing regulatory framework at the international and national level which directly or indirectly applies to AI in the context of liability and development of a rights-respecting responsible AI. Drawing from the best practices of the USA, European Union and China, the paperoutlines the fundamental ethical parameters for AI design. This study seeks to encourage discussion to appraise the readiness of the government, consumers, market, andthe legal framework in addressing the legal, ethical and moral issues surrounding the AI system

Key words: Artificial Intelligence,China, Ethics, European Union, India, Jurisprudential analysis, Legal Personhood, Liability, Regulatory framework, Responsible AI, Sustainable Development Goals, USA

Introduction

In this era of technological revolution, the application of artificial intelligence (AI) has been evidently witnessed in various sectors such as the healthcare, banking and finance, defence and warfare, transportation, navigation, entertainment, legal sector, human resources, education, marketing, manufacturing, and so on. Of the three stages of AI development, we are currently in the transition stage from "Artificial Narrow Intelligence" (ANI or "weak AI" or "narrow AI") to "Artificial General Intelligence" (AGI or "strong AI"), where the AI has not yet achieved the complete range of human-level cognitive, creative and emotional intelligence across all tasks(Price et al., 2018; Spiegeleire et al., 2017). Therefore, due to its limited scope in intelligence, AI underperforms humansin certain tasks (Lukasiewicz & Armour, n.d.). The increasing interaction of the AI system with the human and natural environment, however, requires us to be prepared to address any damage or legal injury resulting from such AI applications. To highlight the importance of addressing liability issues and regulation of AI, let us consider the tele-robotic surgeryperformed by a surgeon controlled remotely from 32 kilometers away(Anvariet al., 2005; Langa, 2018). This example of an AI entity operating under the complete/partial control or supervision of a human highlights the complicacies of assigning liability in cases where there is a malfunction during the actowing to programming errors and/or faulty instructionsby theoperator.

The current regulatory framework at the national and international level is inadequate to address and govern thearray of ethical and legal issues that AI poses today or will pose in the near future.Currently, there is no legal framework governing AI in India. The discussion paper published by NITI Aayog serves as groundwork for formulating a strategic framework at a national level for governing Artificial Intelligence(NITI AAYOG, 2018). As there are no policy guidelines for dealing with AI in India, it may eventually attract legal and ethical issues with regard to its application. Therefore, the need to have a policy framework for businesses (while modelling and coding AI) and the government to meet the legal and ethical standards, can be addressed by primarily

deciding upon the nature of entity an AI system is, and accordingly the liability may or may not be shifted from its creators/operators to the AI system which exercises some degree of self-control.

Based on jurisprudential and sociological constructs and theories, the paper analyses whether conferring of legal personhood upon such AI entities under the Indian law may be appropriate to address liability issues.The paper examines whether AI should be regulated in order to determine issues of liability, and, if so, whether liability may be shifted to the AI entity(exercising some degree of self-control) from its programmers/operators. The paper discusses the existing regulatory framework at the international and national level which directly or indirectly applies to AI in the context of liability issues and development of a rights-respecting responsible AI.Drawing from the best practices of USA, European Union and China, the paperoutlines the fundamental ethical parameters for AI design, applications and regulation which shall underlie such regulatory framework. This study furtherseeks to encourage discussion toappraisethe readiness of the government, consumers, market, and legal framework in addressing the legal, ethical and moral issues surrounding the AI system.

Artificial Intelligence and Models for Determining Liability

Various schemes have been proposed for determining liabilityfor loss resulting from AI applications. One of the most prominent of these schemes byGabriel Hallevydiscusses a three model approach for determining liability of AI, viz., the Perpetration-via-Another Liability Model, the Natural-Probable-Consequence Liability Model and the Direct Liability Model(Hallevy, 2016). Hallevyanalyses, through different situations, as to whether artificially intelligent entities may be able to satisfy the necessary requirements of both actus reusand mens rea (fulfilled either by knowledge, or intention or strict liability - depending upon the offence in question) in order to be held criminally liable.The Perpetration-via-Another Liability modelsuggests that mens reashall be assumed to reside in the software programmer or the AI user for the purpose of determining criminal liability for the wrongful acts of AI,considering the AI to be an innocent agent instrumental in committing such offence.This model is suitable only in cases not involving the advanced capabilities of an AI entity(Majumdar et al., 2019). It is not suitable where the AI entity has committed an offence out of its own 'learnt' experience or knowledge because in such cases, it becomes semi-innocent and not an innocent agent(Lacey et al., 1990). The second model viz., the Natural-Probable-Consequence Liability Model, attributes liability to the AI users or programmers for an offence committed by an AI entity which a 'reasonable' user or programmer ought to have foreseen as a natural and probable consequence of their actions, and should have prevented the same(United States v. Andrews, 1996; State v. Kaiser , 1996). The application of this model may have two possible outcomes: firstly, where the AI entity commits the offence due to negligent use or programming, it cannot be held criminally liable (liability may be determined under the "perpetrator-via-another" model); secondly, where the AI entity acts on its own, in deviation of its programming or use, it shall be held liable. The third model viz., the Direct Liability Model, makes the AI entity liable directly for offences committed by itself, which are not dependent on the programmer or user. Hallevy argues that AI entities should be held criminally liable, similar to humans, if their acts or omissions are capable of fulfilling the requirements of mens rea and actus reus of that particular offence, where such AI entity acted independently of the programmer or user.However, in practice, there may be other stakeholders than the two (programmer and user) mentioned in these three models, such as designers of the hardware parts of the AI entity, hardware manufacturers, maintenance engineers, third parties who may possibly come in contact with such AI entity, and so on (Majumdar et al.2019). In such a scenario, a wrongful act or omission of the AI entity may be a direct or indirect consequence of one or more of these stakeholders' negligent or wilful acts/omissions, rendering the determination of liability in such cases an uphill task using such models (Majumdar et al.2019).

Cerka, Grigiene&Sirbikytesuggest the application of principles such as respondeat superior, vicarious liability and strict liability for determination of AI's liability, by considering the AI as a tool, such that its principal (designer and/or producer) may be made liable for its wrongful act(Cerkaet al., 2015). However, with advanced levels of AI technologies and increased self-control of the AI entity, this model for ascertaining liability may seem unjust where the advanced AI's actions/omissions may be completely unanticipated by the human principal.

Nora Osmaniadvocates for the need of shifting liability from the individual to corporation (AI developers), i.e. corporate criminal liability, in cases where the liability of individual agents cannot be conclusively established(Osmani, 2020). However, this may negatively impact the corporate entity's investment into development of AI. Besides, there is a possibility of events where the harm or damage caused cannot be clearly associated with the programming or operation of AI and affixing corporate criminal liability in such cases may be an unnecessary burden on the corporation. Furthermore, in the absence of a uniform international guiding framework on AI, the acceptability of these AI liability models in various legal jurisdictions which operate on different sets of legal and ethical principles is a matter of debate and discussion.

Giuffrida, Lederer&Vermerysdiscuss three ways of addressing the issue of liability of AI: firstly, AI can be treated as the property of its manufacturer, owner or user; secondly, it may be treated as semi-autonomous; or thirdly, as fully autonomous(Giuffrida et al.,2018). Out of these three models, the first model seems plausible for application in the present world. In the second model, questions regarding whether joint liability principle shall be applied for determining liability of AI, on one hand, and its user or programmer or manufacturer (as the case may be), on the other hand, needs to be considered. This will also necessitate careful assessment of the extent of liability of the joint tortfeasors and/or criminal offenders, as the case may be. The third model cannot be adopted in the present times unless AI reaches such an advanced stage of development where it can be considered fully autonomous by all reasonable means.

Theoretical foundation: Legal personhood, Liability and Ethics

This section focusses on a jurisprudential and sociological analysis of legal personhood, liability, and ethical considerations concerning AI entities.

a) The Theory of Legal Personality

According to eminent philosophers, viz., Gray, Salmond, Pollock and Holland, the theory of legal personality postulates that a legal person is the "subject of rights and duties"(Smith, 1928). Gray states that a will is of essence of a right, which means that without the exercise of will by the right-holder, there can be no right and therefore, no legal personality(Gray, 1921). However, certain human beings (minors and legally incapacitated) and inanimate objects may possess a right and a legal personality without exercising will (Gray, 1921:28). Salmond further explains that in the absence of will, the law attributes the same. Salmond defines a legal person as any being to whom the law attributes "a capacity of interests" and, hence, rights as well as duties(Salmond, 1916). Maitland mentions that a corporation is a living organism with a will of its own(Geldart, 1911). On the same lines, an analogy between AI (which exercises some degree of self-control) and corporations, may be drawn so as to understand the similarity, if any, between how AI, on one hand, and a corporation, as an artificial person, on the other hand, functions. This will enable us to determine the question of legal personhood of an AI entity, and its civil and criminal liability in case of any legal injury arising out of its application in various sectors.

b) Kelsen's Theory of Personality

The attribution of legal personhood has been addressed by Kelsen in his theory of personality, according to which, granting of legal personhood is only a 'technical personification' for the purpose of asserting rights, duties and liabilities(Kelsen, 1945). The theory implies that legal personhood of an entity is, in general, a legal device to organise its rights and liabilities.

c) Hohfeld's Theory of Jural Relations

Based on Hohfeldian analysis of rights, every right has a corresponding duty as its jural correlative. Thus, it is imperative to examine, in the light of jurisprudential analysis of these theories, whether robot rights and liabilities may be rightly asserted by granting them legal personhood. This may, in turn, result in limited liability for the humans concerned with manufacturing/programming/operating the AI system.

d) The Sociological Theory of Distinctive Nature of the Human Species

This theory is of significance in this context. Alan Wolfe discusses that as AI systems are designed to think like a human brain to some extent, it calls for revisiting the proposition laid down by the "sociological theory of distinctive nature of the human species"(Wolfe, 1991). Wolfe emphasises upon the Turing test and its application to check the comparability of machine's intelligence to that of a reasonable human in a given circumstance; and further suggests that it is possible for a machine to replicate a human brain with progress in engineering. (Wolfe, 1991).

e) John Rawls' Theory of Justice

John Rawls proposed theveil of ignorance in his theory of justice,which can be applied to AI systems, whereby AI may be unaffected or lesser affected by human prejudice and emotions in performing its functions (Choudhury &Mulani, 2018). This, however, is majorly dependent on the training data fed into the AI system, which usually reflects the social and cultural biases, thus, perpetuating bias and discrimination in the society (Choudhury &Mulani, 2018). The AI tool should be so designed as to enable it to not only determine what is fair; but also identify, evaluate and correct bias within the parameters laid down by its human-user (Choudhury &Mulani, 2018). This will result in the development of a responsible AI which shall be able to deliver objectively in keeping with the unbiased and ethical standards of an ideal just and fair society.

Artificial Intelligence, Ethics and Bias

The Neo-Luddism movement ascribes to the view that technology is disruptive and has an invasive and dehumanising effect on the society(Gregoire, 2014; Bartlett, 2018). Although Neo-Luddites are not anti-technology, they raise several ethical and moral arguments on the negative role of growing technology in modern society. Kurki&Pietrzykowskidiscuss legal personhood in relation to its legal and moral applications(Kurki & Pietrzykowski, 2017). Alan Wolfe discusses that as AI systems are designed to think like a human brain to some extent, it calls for revisiting the proposition laid down by the "sociological theory of distinctive nature of the human species"(Wolfe, 1991).

Although AI was initially perceived to exhibit human-like intelligence, it may lead to negative outcomes unless it is equipped with human values and ethics. The human mind may, consciously or unconsciously, house social and cultural biases, which reflects in its decisions. Jonnie Penn highlights that despite the fact that machines are engineered to provide outputs with highest standards of accuracy and speed, these machines do not possess the ethics and morale of humans (Penn, 2018). On similar lines, Jeremy Lent argues that AI have no moral or ethical values, similar to that of corporations, and that the development of AI could be a threat to humanity if not controlled in the proper manner(Lent, 2017).However, the AI entities, if trained well, may demonstrate objective and unbiased outcomes, thereby propagating justice and fairness in the society.

Socio-cultural, gender and racial bias in an AI system, which may be rooted in the programming or training data, consciously or unconsciously originating from the software developer or programmer/coder, has a significant bearing on the output of an AI system(Barr, 2015; Chen, 2009).Bavitz, Weber & Jonesemphasise upon the importance of risk-assessment software applications to check against the presence of bias in the criminal justice administration(Bavitz, Weber, & Jones, 2017). It is claimed, for instance, that marginalised groups are treated in a biased manner by the judges. In such cases, a risk assessment tool can aid in assessing the risk, if any, that an accused person poses in a given situation, thereby achieving better objectivity in decision-making by the judges by limiting their exercise of discretion, and hence, reducing or eliminating bias. However, these tools are programmed by humans and trained using large datasets. In the presence of any programming errors or bias in the training data, the output from such software will also be erroneous, thereby increasing the risk to injustice if relied upon in the courts Therefore, an extensive research and discussionconcerning the resolution of the issue of bias and discrimination in the AI system, and, in general, the ethical parameters for AI designing, operation and regulation is crucial.

Ethical standards for AI in USA, China and EU

There are several global leaders in AI technologies, however, for the purposes of this study, the author shall focus on the United States, China and the European Union.The United States has, in addition to adoption of OECD and G20 AI Principles in 2019(The White House), also launched 'American AI Initiative', a five-pronged national strategy on artificial intelligence, which, inter alia, focusses on setting AI governance standards so as to promote reliable and trustworthy AI, foster public trust in AI and also protecting civil liberties and privacy(Office of Science & Technology Policy, 2019). In January 2020, 'AI Regulatory Principles' have been proposed by the White House for application in private sector aimed at public engagement, trustworthy AI and limiting regulatory overreach(The White House). Further, several Bills have been introduced such as the SELF DRIVE Act, 2017(concerned with informing consumers of capabilities and limitations of highly autonomous vehicles), the House Resolution 153 (to govern ethical implications of AI), the FUTURE of Artificial Intelligence Act, 2017 (to establish advisory committee on development and implementation of AI), Algorithmic Accountability Act, 2017 (to conduct impact assessment of automated decision system and data protection)(AI Policy – United States: AI in Congress: BAAI).China introduced the 'Beijing AI Principles' in May 2019 consisting of 15 principles divided into three sections, viz. Research and Development, Use, and Governance; aimed at fostering respect for privacy, dignity, autonomy of rights, justice and fairness, inclusivity and openness, freedom, safety and security(AI Policy- China: BAAI).The European Union published "Ethics Guidelines for Trustworthy Artificial Intelligence" in April 2019, emphasizing that for an AI to be trustworthy it must be lawful, ethical and robust(European Commissson , 2019). These guidelines also laid down seven key requirements for a trustworthy AI. Further, the "European Commission for the Efficiency of Justice" (CEPEJ) has adopted the "European Ethical Charter on the Use of AI in Judicial Systems and their Environment" in December 2018 which consists of 5 principles, viz., "respect for fundamental rights, non-discrimination, quality and security, transparency, impartiality and fairness and under user control" (informed users exercising control over their choices)(European Commission, 2018).

At present, the AI does not possess moral values alike of a human, and the functionality of the current AI applications are mostly independent of the presence or absence of moral values. This means that the processing of the output does not require AI to apply moral values although its output may be affected by the nature of values embedded into it through training data or programming. As we progress to the advanced stages of AI, AI applications may be trained to respect ethics and morals, and it may 'learn'to apply the same while processing its outputs. However, as ethics and morals are highly subjective and varies from individual to individual and across geographical regions, it will be interesting to see how embedding of values into an AI system which exercises complete or partial self-control, would affect its output, and its resulting legal implications.

Regulatory Framework Governing AI Applications

The existing regulatory framework at the national and international level is inadequate to address and govern the array of ethical and legal issues that AI poses today or will pose in the near future.The relevant regulatory framework which directly or indirectly applies to AI in the context of liability issues and development of a rights-respecting responsible AI is discussed below:

i) The UN Convention on the Use of Electronic Communication in International Contracts, 2005

Article 12 of the "UN Convention on the Use of Electronic Communication in International Contracts", 2005 recognizes validity and enforceability of contracts formed as a result of actions by automated message systems (electronic agents), even if no natural person reviewed each of the individual actions carried out by the systems or the resulting contract. In such cases, liability of the principal (human) and agent (automated message systems) becomes difficult to be determined with regard to third party, in case there is a fault on the part of the electronic agent. Secondly, predictive technology is used to determine whether bail is to be granted or not, based on the likelihood of recidivism and appearance in court. However, this involves the risk of perpetuating human bias (based on gender, occupation, financial and societal status, etc.) through the AI, if it is not programmed in an unbiased manner.

ii) The United Nations Guiding Principles on Business and Human Rights, 2011

The UN Guiding Principlesserve as a global standard of obligations of the State (Principles 1 to 10) and business enterprises (Principles 11-24) to protect human rights, and guidelines on howto assess,prevent and address human rights abuse linked to business activities. Principle 15 defines the parameters of human rights due diligence, and Principles 18-21 describe its components. The UN Guiding Principles can be applied to the development of AI by businesses by requiring them to observe 'human rights due diligence' when deploying and developing AI technologies to check against human rights abuses. These Principles also require the State to ensure adequate laws, in compliance with their internationalhuman rightsobligations (Principle 5), and access to effective remedy (Principle 25)in case ofadverse human rights impacts of AI.

iii) OECD Principles on Artificial Intelligence, 2019

The OECD AI Principles lay down the first intergovernmental standard, consisting of five value-based principles, while promoting innovative and trustworthy AI that respects democratic values, human rights and rule of law. These complement existing OECD standards relating to digital security risk management, privacy, responsible conduct in businesses, and have been adopted by OECD member countries and other ountries as well.

iv) G20 AI Principles, 2019

The G20 AI principles, which has been adopted by G20 members, promote responsible and trustworthy AI based on human-centered values,and have been drawn from the OECD Principles and recommendations.

Position in India

India, unlike USA, EU or China (as discussed above) does not yet have a dedicated legislative or regulatory framework to specifically deal with AI technology related issues.The discussion paper published by NITI Aayog serves as groundwork for formulating a strategic framework at a national level for governing Artificial Intelligence(NITI AAYOG, 2018). The relevant existing constitutional,statutoryand tort law provisionsin relation to data protection, product liability, patenting rights, etc. are discussed below.

i) The Constitution of India

The 'right to life and personal liberty' under Article 21 of the Constitution has been interpreted by the Indian judiciary to include within its ambit several fundamental and indispensable aspects of human life. In the leading case of R Rajagopal v. State of Tamil Nadu, the right to privacy was held to be implicit under Article 21 of the Indian Constitution. The tort law also provides for damages for unlawful invasion of privacy. This judgement is relevant with regard to addressing privacy issues arising out of growing use of AI in processing personal data. Further, in the landmark case of K.S. Puttaswamy v. Union of India, the Supreme Court emphasised upon the need for a comprehensive legislative framework for data protection, which shall be competent to govern emerging issues such as the use of AI in India. Protection of data is linked to the right to privacy and confidentiality which draws its source from Article 21 of the Constitution. Further, the AI may sometimes be completely fair and objective yet inequitable in its approach (Majumdar et al. 2019). It is understood that bias may creep into the AI system if it is not designed effectively and then the AI can perpetuate the bias and discrimination in its operations (Choudhury &Mulani, 2018). In such situations, Articles 14 and 15, which deal with the right to equality and right against discrimination respectively, are relevant in this context to provide protection of these fundamental rights.

ii) The Patents Act, 1970

The main issues concerning AI and patent law are: firstly, patentability of AI, secondly, inventorship, i.e., interpretation of "true and first inventor"; and thirdly, ownership and liability for AI's acts/omissions(Soni & Singh, 2019). For the purpose of this study which examines the issues of legal personhood and liability of AI, the author shall focus on the second and third issues named above. Section 6 of the Patents Act, 1970 provides that a patent application for an invention can be made by a 'person' claiming to be its "true and first inventor". Section 6 read with Section 2(1)(y) of the Act does not specifically mandate that 'person' must be a natural person, although that is conventionally understood or assumed to be so. At present, unlike Saudi Arabia, AI has not been granted legal personhood in India(Hart, 2018), however, with regard to AI-generated inventions sans human intervention (as in the case of two inventions claimed to be autonomously invented by the AI machine DABUS in UK)(Abbott, 2019), it is pertinent to see whether AI may be granted legal personality in the times ahead and, whether 'person' under the patent law might include AI as an inventor (although the ownership of the patent may lie with a human)(The Economic Times, 2019). Taking into consideration the heuristic nature of AI technologies(The Economic Times, 2019) and their ability for independent decision-making and problem-solving(EPO, 2020), to make humans responsible for AI's all such unprecedented acts or to give humans the credit for AI-generated inventions sans human intervention may not be justifiable, and the latter may devalue the integrity of the patent ecosystem (Abbott, 2019). Another concern which arises is that in case of patent infringement owing to AI's actions not linked to a human actor, whether the liability will be imposed upon its operator, owner or the AI entity itself, and, to what extent. Therefore, the Indian patent regime needs to be updated to provide clear guidelines to determine inventorship for such inventions to ensure, on one hand, software related research, investments and innovations are encouraged (Sony & Singh, 2019: 103), and on the other, the liability for patent infringement is balanced to rightly allocate responsibility for AI's wrongful acts/omissions.

iii) The Personal Data Protection Bill, 2019

This Bill seeks to regulate the processing of personal data of Indian citizens by public and private bodies located within and outside India. It emphasizes upon 'consent' for processing of such data by data fiduciaries, subject to certain exemptions. This Bill, if enacted into law, will significantly affect the wide application of AI software which collects user information from various online platforms to track user habits relating to purchase(Paul, 2020; Morgan, 2018) or online content(Chaslot, 2019; NOVATIO, 2018; Gavira, 2018) or finance(Bachinskiy, 2019; Desai, 2016), etc.

iv) The Information Technology Act, 2000

Section 43A of the Information Technology Act, 2000 imposes liability on a body corporate, dealing with sensitive personal data, to pay compensation, when it fails to adhere to reasonable security practices. This has significant bearing in determining liability of a body corporate when it employs AI to store and process sensitive personal data.

v) The Consumer Protection Act, 2019

Section 83 of the Consumer Protection Act, 2019 entitles a complainant to bring an action against a manufacturer or service provider or seller of a product, as the case may be, for any harm caused to him on account of a defective product. This establishes liability for the manufacturer/seller of an AI entity for harm caused by it.

vi) Relevant principles under the Law of Torts

Besides the statutory provisions, some principles from the uncodified tort law are also relevant in this context. The principles of vicarious liability and strict liability are relevant to the determination of liability for wrongful acts or omissions of AI. Some other relevant principles which may be applicable in this regard are remoteness and foreseeability of damages and control test in the context of vicarious liability. In SitaramMotilalKalal v. SantanuprasadJaishankar BhattA.I.R. 1966 S.C. 1697 (India), the court held that the principal will be liable for a

wrongful act of his agent if the act is done under the actual control of the principal. Further, in the case of Harish Chandra v. EmperorA.I.R. 1945 All. 90 (India), the court laid down that there is no vicarious liability in criminal law as one's mensrea cannot be imputed to another, unless the legislature provides otherwise. These judgements have a bearing upon determination of liability for AI's wrongful acts if the AI entity may be considered an agent of the human operator.

Thus, it is submitted that, as the cutting edge AI technologies open a whole gamut of opportunities and threats, and are very distinct from the hitherto existing technology, it is pertinent to make necessary amendments to existing laws while taking into account the AI applications and the possible concerns arising therefrom.

6. Conclusion and Suggestions

At present, although AI applications do not employ the optimum level of automation where AI can operate in a fully autonomous mode without human intervention such as the autonomous inventions by the AI machine DABUS in UK (Abbott, 2019), it will be rather sooner than later when, with the deployment of highly advanced levels of automation involving independent decision-making and heuristic problem solving, we may have to consider a shift from application of product liability or vicarious liability or strict liability principles to direct liability models for assigning liability for AI's wrongful acts or omissions.However, even at this stage where numerous AI applications are carried out under human supervision, the illustrations discussed earlier (relating to self-driving car and tele-robotic surgery) bring to light the complexity of assigning liability as several stakeholders are involved and responsible inputting the whole system together,related to the designing, supply of hardware, programming, installing sensors, operation and maintenance, designing business policies for overseeing theoperation process,ensuring legal compliances, and so on (O'Kane, 2018).As the cutting edge AI technologies open a whole gamut of opportunities and threats and are very distinct from the hitherto existing technology, it is pertinent to make necessary amendments to existing laws while taking into account the AI applications and the possible concerns arising therefrom. Therefore, in order to ascertain liability and award compensation for wrongs committed by AI entity, the author highlights the need for a policy framework which should take into consideration certain ethical and legal parameters, as discussed above.

In the light of the preceding discussion and analysis, the author enlists the following suggestions:

i) Determination of liability and legal personality of AI

At different stages or tiers of AI development, the models for liability determination may vary and have to be suitably adopted. For instance, in the first stage, i.e. ANI, where the AI has not achieved the complete range of human-level cognitive, creative and emotional intelligence across all tasks, the liability for AI's wrongful acts could rest on its operator or software programmer or manufacturer, as the case may be, depending on the proximate cause of the wrongful act. In the second stage, i.e. AGI, where the AI's intelligence equals to that of a human across all tasks, the elements of intention, knowledge and negligence should be given due consideration in determination of liability for AI's actions. If the wrongful act of the AI is caused due to error or negligence in operation or programming of the AI system or unlawful interference by any third party, the operator or programmer could be assigned liability. On the other hand, if the AI system acts on its own, in defiance of its programming or operator's instructions, the AI could be held liable. In the final stage, i.e. ASI, where the AI exceeds human-level intelligence across all tasks, the AI could be held liable for its wrongful acts committed out of its own volition, independently of its user or programmer, and in the absence of any unlawful interference by any third party. In all such situations where liability could be imposed on the AI, for reasons mentioned above, conferring the AI with legal personality will be essential.

In consideration of the current stage of AI development and applications (i.e. ANI), it is suggested that granting of legal personality to AI may not be appropriate at this juncture, instead AI may be considered to be an 'agent' of its human operator. Consequently, to ascertain liability for AI's wrongful acts or omissions, the principal (the

operator under whose command the AI operates) shall be liable under the principles of vicarious liability or strict liability under Law of Torts, while the manufacturer may be liable under product liability under Consumer Protection Act in case of a manufacturing defect. With regard to determination of liability, Gabriel Hallevy discussing three pronged approach of addressing the criminal liability of AI. However, taking into account the primary objectives of criminal law and civil law, viz., punishment and compensation respectively, compensation may be better suitable in the current stage of AI development, with insistence upon institution of an insurance fund to serve as an available repository for redressing wrongs committed directly or indirectly by AI's acts or omissions.

ii) A right-respecting comprehensivepolicy guidelinefor responsible AI encompassing multi-stakeholder interests and liability

A comprehensive rights-respecting strategic framework encompassing multi-stakeholder interests and liability needs to be designed to address the legal, ethical and moral implications of AI technologies. The different stakeholders involved may include those responsible for designing the car, supply of hardware, programming, installing sensors and designing company policies for overseeing the driving process, as well the end-user and the Government responsible for regulation and oversight.A clear and comprehensive policy framework shall be designed based on the parameters of a responsible and trustworthy AI. The guidelines shall govern the stages of AI designing, programming, assembling, training, operating, maintenance and any other intermediate stage which has a bearing on the way AI entity 'thinks' and functions. This is necessary to be observed that at every stage, due diligence is observed by the several stakeholders involvedto ensure respect and protection for right to privacy or right against discrimination, or right to safety and a multitude of such other rights entitled to a human being.

iii) Ethical parameters for a trustworthy and responsible AI

Based on the analysis of the interviews as well as a study of the legislative and policy frameworks in USA, EU and China, the author considers certain ethical parameters to be paramount for the policy framework for India, viz., protection and respect for rights and freedoms such as equality, privacy, safety, human life and dignity, security, data protection, right against discrimination. The NITI Aayog has discussed that the AI system needs to be designed on the lines of FAT (Fairness, Accountability and Transparency) framework.

iv)Protection and respect for rights in compliance with international standards

In appraisal of the existing and potential future implications, both positive and negative, of AI on human rights and freedom, the author suggests that the protection and respect for rights shall be observed in compliance with not only the Indian legislative framework but also the international instruments (such as the International Bill of Rights and other Conventions/treaties which India has ratified) in a robust manner.

v) Strengthening the data protection regime

The AI technology is trained and operatedbased on user personal data in large volumes, which in turn, poses significant potential threats concerning any illegal or unfair or non-consensual use of user's personal data by AI programs. The Indian legislative framework for protection of personal data (Personal Data Protection Bill, 2019) has not yet been enacted into law.Therefore, a strong data protection regime, drawing from the best practices under the EU General Data Protection Regulation (GDPR),competent to govern emerging issues surrounding the use of AI in Indiais highly imperative.

vi) Setting standard guidelines for the State and businesses dealing with AI

A set of standard guidelines reflecting upon the role of government and businesses in capacity-building and designing techno-legal regulatory policies is important. The companies engaged in modelling, assembling,

training or overseeing operations of AI share a great deal of responsibility in ensuring a rights- respecting AI. Thus, there is a need to establish standard legal and ethical guidelines for businesses regarding dealing with AI in all such stages as mentioned above. Similarly, the Government has a very important role to play with regard to monitoring the observance of such framework, and penalizing for contravention.

vii) Constitution of an Insurance Fund for compensation of wrongs

The constitution of an insurance fund will be beneficial as it may serve as an available repository for redressing and compensating for wrongs committed directly or indirectly by AI's acts or omissions, which may be either foreseeable or unforeseeable.

viii) Regular and periodical monitoring by aninterdisciplinary expert team

It is suggested that regular and periodical monitoring by experts from the field of technology and law working in collaboration is desirable to check and ensure that the functioning of the AI system is in adherence to all the above mentioned legal and ethical parameters as well as rule of law.

References

1. Accelerating America's Leadership in Artificial Intelligence. (2019, February 11). Retrieved from Office of Science and Technology Policy, The White House: https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/

2. AI for American Industry. Retrieved from The White House: https://www.whitehouse.gov/ai/ai-american-industry/

3. AI Policy – United States: AI in Congress. Retrieved from Future of Life Institute: https://futureoflife.org/ai-policy-united-states/

4. AI with American Values. Retrieved from The White House: https://www.whitehouse.gov/ai/ai-american-values/

5. Anvari, M., McKinley, C., & Stein, H. (2005, March). Establishment of The World's First Telerobotic Remote Surgical Service: For Provision of Advanced Laparoscopic Surgery in A Rural Community. Annals of Surgery , 241(3), pp. 460-464. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1356984/#:~:text=The%20first%20telerobotic%20surgery%20was,City%20on%20September%207%2C%202001.&text=Although%20the%20%E2%80%9CLindbergh%20operation%E2%80%9D%20was,routine%20use%20of%20this%20technology.

6. Barr, A. (2015, July 2). Google Mistakenly Tags Black People As 'Gorillas', Showing Limits of Algorithms. Retrieved from The Wall Street Journal: blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/

7. Bartlett, J. (2018, March 4). Will 2018 Be the Year of the Neo-Luddite? Retrieved from The Guardian: https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite

8. Bavitz, C., Weber, G., & Jones, D. (2017, December 1). When a Bot is the Judge, . Retrieved from Berkman Klein Center for Internet and Society, Harvard University: https://cyber.harvard.edu/podcast/when-a-bot-is-the-judge

9. Beijing Academy of Artificial Intelligence (BAAI). (n.d.). AI Policy – China. Retrieved from Future Of Life Institute: https://futureoflife.org/ai-policy-china/

10. Cerka, P., Grigiene, J., & Sirbikyte, G. (2015). Liability For Damages Caused By Artificial Intelligence. Computer Law & Security Review, 31 , 376-389.

11. Chen, B. X. (2009, December 22). HP Investigates Claims of 'Racist' Computers. Retrieved from Wired : https://www.wired.com/2009/12/hp-notebooks-racist/

12. Chowdhury, R., & Mulani, N. (2018, October 24). Auditing Algorithms for Bias. Harvard Business Review . Retrieved from https://hbr.org/2018/10/auditing-algorithms-for-bias

13. Discussion Paper: National Strategy for Artificial Intelligence. (2018, June). Retrieved from NITI AAYOG: https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf?utm_source=hrintelligencer

14. Emerging Technologies. (2018, November). Retrieved from Internet Governance Forum, UnitedNations: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6037/1412.

15. Geldart. (1911). Legal Personality . Law Quarterly Review, 27, 93.

16. Giuffrida, I., Lederer, F., & Vermerys, N. (2018). A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law. Case Western Reserve Law Review, 747. Retrieved from https://scholarlycommons.law.case.edu/caselrev/vol68/iss3/14

17. Gray, J. C. (1921). The Nature and Sources of the Law (2nd ed.). (R. Gray, Ed.) New York : Macmillan.

18. Gregoire, C. (2014, January 17). A Field Guide to Anti-technology Movements, Past and Present. Retrieved from The Huffington Post: https://www.huffingtonpost.in/2014/01/17/life-without-technology-t_n_4561571.html

19. Hallevy, G. (2016, March). The Criminal Liability of Artificial Intelligence Entities – From Science Fiction to Legal Social Control. Akron Intellectual Property Journal , 4(2). Retrievedfrom http://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1037&context=akron

20. Kelsen, H. (1945). General Theory of Law and State . Harvard Univeristy Press.

21. Kurki, V. A., & Pietrzykowski, T. (2017). Legal Personhood: Animals, Artifiicial Intelligence and the Unborn. Cambridge , UK: Springer.

22. Lacey, N., Wells, C., & Meure, D. (1990). Reconstructing Criminal Law: Criminal Perspectives on Crime and the Criminal Process (2d ed.). London , UK: Weidenfeld and Nicolson. Retrieved from http://eprints.lse.ac.uk/id/eprint/5592

23. Langa, M. (2018, December 6). Ahmedabad Doctor Performs Telerobotic Surgery on Patient 32km Away. Retrieved from The Hindu: https://www.thehindu.com/news/national/other-states/ahmedabad-doctor-performs-telerobotic-surgery-on-patient-32-km-away/article25675166.ece

24. Lent, J. (2017, December 1). AI Has Already Taken Over, It's Called the Corporation. Retrieved from Counterpunch: https://www.counterpunch.org/2017/12/01/ai-has-already-taken-over-its-called-the-corporation/

25. Levin, S. (2016, December 15). Uber Blames Humans for Self-Driving Car Traffic Offenses as California Orders Halt. Retrieved from The Guardian: https://www.theguardian.com/technology/2016/dec/14/uber-self-driving-cars-run-red-lights-san-francisco

26. Levin, S., & Wong, J. C. (2018, March). Self-Driving Uber Kills Arizona Woman in First Fatal Crash Involving Pedestrian. Retrieved from The Guardian: https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe

27. Lukasiewicz, T., & Armour, J. (n.d.). AI for English Law - Work Package Three - Frontiers of AI in Legal Reasoning. University of Oxford. Retrieved from https://www.law.ox.ac.uk/research-and-subject-groups/ai-english-law-work-package-three

28. O'Kane, S. (2018, May 7). Uber Reportedly Thinks Its Self-Driving Car Killed Someone Because It 'Decided' Not to Swerve. Retrieved from The Verge: https://www.theverge.com/2018/5/7/17327682/uber-self-driving-car-decision-kill-swerve

29. Osmani, N. (2020). The Complexity of Criminal Liability of AI. Masaryk University Journal of Law and Technology, 14(1), 53-82. Retrieved from https://doi.org/10.5817/MUJLT2020-1-3

30. Penn, J. (2018, Novemeber 26). AI thinks like a corporation—and that's worrying. Retrieved from The Economist : https://www.economist.com/open-future/2018/11/26/ai-thinks-like-a-corporation-and-thats-worrying

31. Price, L. C., Walker, L. S., & Wiley, C. W. (2018). The Machine Beneath: Implications of Artificial Intelligence in Strategic Decision Making. PRISM- The Journal of Complex Operation , 7(4), 96. Retrieved from www.jstor.org/stable/26542709

32. Priyanka Majumdar et al. (2019). Artificial Intelligence, Legal Personhood and Determination of Criminal Liability. Journal of Critical Reviews , 6(6), 323-325. Retrieved from http://www.jcreview.com/?mno=302645189

33. Salmond, S. J. (1916). Jurisprudence (5th ed. ed.).

34. Smith, B. (1928). Legal Personality. Yale Law Journal , 37(3), 283. Retrieved from http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=3259&context=ylj

35. Spiegeleire, S. D., Maas, M., & Sweijs, T. (2017, January). Artificial Intelligence and the Future of Defense: Strategic Implications for Small and Medium-Sized Force Providers. Hague Centre for Strategic Studies, 30. Retrieved from www.jstor.org/stable/resrep12564

36. State v. Kaiser , 918 P. 2d 629 at 245 (Kan. 1996).

37. United States v. Andrews, 75 F. 3d 552 (9th Cir. 1996).

38. Why Uber's Self-Driving Car Killed a Pedestrian. (2018, May 29). Retrieved from The Economist: economist.com/the-economist-explains/2018/05/29/why-ubers-self-driving-car-killed-a-pedestrian

39. Wolfe, A. (1991, March). Mind, Self, Society and Computer: Artificial Intelligence and the Sociology of Mind. American Journal of Sociology, 96(5), 1073-1096.