May 19, 2020

Indian Strategy for AI & Law, 2020

INDIAN SOCIETY OF ARTIFICIAL INTELLIGENCE & LAW™

#AIforNewIndia

Preliminary Recommendations
May 2020

Contributed by:
Ananya Saraogi, **Research Intern**
Manohar Samal, **Research Intern**
Nayan Grover, **Research Intern**
Sameer Samal, **Research Intern**
Vedant Sinha, **Research Intern**
Vaishnavi Venkatesan, **Research Intern**
Vedant Sinha, **Research Intern**

Approved by: Abhivardhan,
Chairperson & Managing Trustee

Indian Strategy for AI & Law, 2020

#AIforNewIndia

Preliminary Recommendations
May 2020

For any correspondence queries, do not hesitate to contact us at editorial[at]isail[dot]in

Send us letters N/O Indu Bala Srivastava,
8/12, Patrika Marg, Civil Lines, Prayagraj (Allahabad), India - 211001

You can cite the recommendations report using the IEEE/ISO 690 format. Kindly refer to citethisforme.com to cite properly or Microsoft Word if you a Windows User.

INDIAN
SOCIETY OF
ARTIFICIAL
INTELLIGENCE &™
LAW

About

The Indian Strategy on AI and Law (ISA) is our policy project under the Indian Society of Artificial Intelligence and Law, where we intend to enlighten and discover various avenues of AI Ethics and Law in its multidisciplinary content, and devise solutions for the Indian Economy through policy recommendations, internship programmes and academic conferences.

The Executive Council of the Indian Society of Artificial Intelligence & Law has mandated the production of the Indian Strategy on AI and Law (ISA), 2020, which we intend to submit to various stakeholders in the AI Ethics and Law ecosystem present in India, which includes various state and non-state actors.

We hope that by **December 2020**, we would come up with a comprehensive policy draft that guides for a vibrant and intelligible New India!

Thank you.

Abhivardhan
Chairperson &
Managing Trustee

Areas of Research Under Recommendation

1 Artificial Intelligence and Commercialization of Outer Space

Research Area: AI, Ecology & Space Studies.

2 Civilian and Military Environments & the Compliance of AI

Research Area: Artificial Intelligence & Constitutionalism.

3 Legal Personhood of Artificial Intelligence

Research Area: Artificial Intelligence and Constitutionalism

.

4 Artificial Intelligence in Corporate Transactions: AI, Automated Mergers & Acquisition and Corporate Ethics

Research Area: Artificial Intelligence and Corporate Governance.

5 Artificial Intelligence and Privacy

Research Area: Artificial Intelligence and Constitutionalism.

6 Machine Learning and Privacy Mechanisms in India

Research Area: Artificial Intelligence and Constitutionalism.

7 Artificial Intelligence and Intellectual Property: Collateral Parallelism

Research Area: Artificial Intelligence and Intellectual Property Law.

Recommendations Published on May 19, 2020.

Recommendations on: Artificial Intelligence and Commercialization of Outer Space

Research Area: AI, Ecology & Space Studies

Manohar Samal[1]

[1] Research Member, Indian Society of Artificial Intelligence and Law

- The vision of commercial space activity in India is not a newfound phenomenon and has already been introduced through the Space 2.0 phase which is currently dedicated to enable space entrepreneurs, small and medium scale enterprises to compete in the commercial space race which is worth $300 billion dollars. Evidence of the origin of commercial space activities can be traced to the year 1992, which was when Antrix Corporation Limited, a company owned by the Indian Government was established. The Pragyan Rover launched with Chandrayaan- 2 is one of the most successful artificial intelligence rovers launched by India and showcases the potential of artificial intelligence in space missions.
- Some of the areas where artificial intelligence can contribute in enhancing space commercial activities in India are improved risk assessment of projects, progress in data collection, analysis, transmission, mapping and management, efficacious manufacture and development of space products such as spacecrafts, rockets, probes, rovers, space suits and telescopes, technology capacity building, efficient launch and landing, improvement in mission success rates, indulgence in commercial remote sensing, prolonged space travel, simulated training for astronauts, improved mission support systems, amelioration of services in India like geospatial positioning, internet and telecommunications and some long term goals such as asteroid mining and space tourism.
- In order to ensure the successful application of artificial intelligence in commercial space activities, it is extremely vital that a central space law is passed. Such law would have to preliminarily stipulate the areas of commercial space in which private enterprises can contribute and the areas in which they are restricted, provide guidelines for jurisdiction over space objects and discoveries, envisage clear principles of liability and a penal structure mechanism. It is indisputable that in the initial decades of the operation of such law it will not be possible to accommodate fully privatised space commercial activities and supervision will require to be strict in order to facilitate sustainable and orderly utilisation of commercial space. In view of the fact that space activities involve country responsibility, a critical effect on diplomatic and international relations and impact on the planet itself, it is pertinent that the penal mechanism inculcated within an Indian space law will have to be closely connected to Indian criminal jurisprudence and will have to create a "right in rem". It is

noteworthy that in the absence of these elements in a codified space law, basic activities will not occur smoothly and the application of artificial intelligence might not bring out the best results.

- After achieving the first step of implementing a resilient, all- embracing and coherent central space law, public- private partnership would have to be embraced within the provisions of such law. Several applicable public private partnership models and a model concession agreement to cater the relationship between the public and private sector will have to be formalised. Although the Indian Space Research Organisation has already floated a tender in the year 2017, after the adoption of a central space law, the volume of operations will significantly rise and the present structure will then be rendered insufficient. For increased development and usage of artificial intelligence in these activities, a partnership with technology based, robotics and artificial intelligence development companies will have to increase. Incentive schemes have been one of the most successful methodologies to attract investment and partnerships in any sector in India which has included tax and duty waivers, partial and absolute, land allocation and government grants. Attraction of investors and constructive public private partnerships between artificial intelligence tech- companies and the Indian Space Research Organisation can lead to the positive development of enhancement in manufacture and innovation of space products such as spacecrafts, rockets, probes, rovers, space suits and telescopes that will significantly boost the duration of space travel and its activities, ensure advancements in remote sensing and other services .
- The Indian Space Research Organisation has already employed artificial neural networks in mission support systems and the collection, analysis, transmission, mapping and management of data. It is pertinent that artificial intelligence is also used for the improvement of simulated training of astronauts, risk assessment and analysis, which can result in progress of the mission success rate of the targeted commercial space activity. Softwares using artificial intelligence algorithms such as Space Mission Architecture and Risk Analysis Tool (SMART) are already being used for conducting risk analysis and assessment. Furthermore, Visual Environment for Remote Virtual Exploration (VERVE) is one of the training simulation platforms for astronauts. Therefore, it is trite that capacity building in artificial intelligence technology forms the crux of how progress can be achieved in these activities. Bilateral treaties that emphasise upon import of artificial intelligence technology for commercial space activities can prove to be resourceful for capacity building. However, it is necessary that simultaneous indigenous development is also facilitated and catered so that dependency rates do not remain extremely high in the upcoming decades.
- It is significant that law and policy- making is rethought for the purposes of commercial space activities. This is because the rise in such commercial activities in space will inevitably result in the development of new professions and the increase in space travellers that will not essentially be astronauts. The role of artificial intelligence will be extremely high as more virtual reality based simulations will be used for the rigorous training of such non- astronaut space travellers.
- Another key aspect which a central space law would have to emphasize on is the distinction of regulations between autonomous and manned missions. A host of

delegated legislation that include procedures for registration, mission supervision and licensing. In order to ensure the development and increment of space exploration and sub- orbital activities, it is pertinent that the application of artificial intelligence is also explored in robotics to create autonomous space products such as autonomous rovers, landers and probes. Simplification of procedure in attaining reciprocal treatment of intellectual property rights of existing artificial intelligence based space products and a robust mechanism that permits the ownership of certain specified space objects on discovery by private entities is capable of magnifying the amount of autonomous commercial space activities from India. The magnification of commercial space activities in India will also result in the indulgence of private entities in constructing launch pads and therefore, in order to avoid the incoherent construction and development that affects Master Plans of urban and rural development has to be regulated.

- Increased usage of the latest 3D printing tools and the benefits under the “Make In India Scheme” can significantly aid in the reduction of manufacture, operation and ultimately, the overall mission costs. Indian space missions are already popular for being cost- effective and is also considered as one of the best nations who is capable of efficiently launching nano and mini satellites. However, the central space law will have to address certain challenges to ensure that all types of commercial space activities are cost- effective and ecological. Since space law is not concretely codified in India till today, its formulation can mandate manufacturers to research, develop and utilise clean and sustainable technology to build space products that reduce prices. Application of Space Based Solar Power (SBSP), reusable space vehicles, better payload management, efficient Power Management and Distribution (PMAD) and energy storage systems are few of the clean technology methods that can be mandated as “basic standards” for Indian based space products. Moreover, a space regulatory agency will have to be established which not only will regulate the private sector in India but will also regulate exports of Indian manufactured space products to other nations of the Global South. Furthermore, the national agency can also be entrusted to provide training to other Global South nations and also, create guidelines for Indian partnerships with other nations to launch their products into outer space.
- Presently, a legal framework for space tourism and asteroid mining may not be conducive since India may be quite a lot of decades away from indulging in such activity. However, at the same time a resilient framework that accommodates a strong support system and services and participation towards other nations of the Global North that are closer towards achieving this goal can certainly act as a catalyst to speed up the process in India.
- It is not unreasonable to infer that a commercial space race may lead unsustainable activities that harm space objects and the whole planet itself and therefore, it is extremely vital to stringently and manifestly formulate and implement policies that will facilitate and promote sustainable commercial space activity and sustainable exploitation of space resources.

Recommendations on: Civilian and Military Environments & the Compliance of AI

Research Area: Artificial Intelligence and Constitutionalism

Vedant Sinha[1]

[1] Research Member, Indian Society of Artificial Intelligence and Law

- Clive Humby coined the phrase, that “Data is the new oil”, however Lt. Gen Jack Shanahan feels differently, that it is “a mineral ore, there’s a lot of crap. You have to filter out the impurities from the raw material to get the gold nuggets”. The enormous amounts of data flowing within the physical infrastructure can be mostly non-consequential at face value, however when purified, it holds value, thereby forming one of the stress point in usage of AI, the dependability on the quality of the dataset. Therefore, the methods to purify the data are as important as the AI, it is being fed, based on AI gullibility.
- AI is very gullible, amid pattern recognition the minutest of impurities data can consequentially change the nature and the results of the AI, so much that the deviation due to outliers, missing values or can alter the projected results. A large set of clearly labelled, well-organized data points is what machine learning algorithms need to learn from before they can try making sense of raw data the humans haven’t cleaned up for them.
- In a military setting, the AI must be robust. For a robust AI to work in a surveillance situation, for example, to differentiate between a Civilian and a militant, it has to first understand the difference between what is normal and abnormal behaviour for a civilian and to do the same, it has to train on a wide assortment of civilian data, to establish a range of normality and abnormality. However, privacy concerns do arise and the Constitutional Courts can deprive the access to data per the privacy concern, deprives the military of relevant datasets to utilise. There the balance between the private data of a person is of National security consequence or not, has to be demarcated or even if this operation has to be performed or not. Doing it provides the state legitimacy to claim sovereign immunity under Tort Law.
- The lines get blurrier in a warzone, where the citizen is often not hostile, but not cooperative with the occupational forces as well, and the data-points extracted from a set of co-operating citizen mindful of the law is different from those civilians whose rights and its co-relatives are altered in a warzone. Thereby different standards for AI arise in both peaceful and warzone situations and even within this scenario, there exists a probability for Algorithmic Bias to exist. Therefore, AI may be trained in a normal situation might probably tag normal civilians in warlike situations as militants.

- It is not only sufficient to be able to conclusively segregate militants from a normal citizen, in a peaceful or a warzone scenario. It is equally important for the AI to delineate the explanations for the outcome achieved and answer questions such as "why", "how" of such classifications.
- Explainability of the AI employed in the military should be a big factor under consideration, and such models such be employed that does not morph into a Blackbox. Any such solution that seeks to unravel the reasoning such as deep explanation or model induction only does as a predictive, not an affirmatory solution.
- If the AI decides to tag an individual, then the right of authorisation to execute an action, in that case, should still reside with a Human operator as a safety valve against any mistake that the AI might commit.
- If the human operator relies on the AI to execute a decision, then the liability in such a scenario might not rest upon AI, as the human operator had the chance to exercise due diligence. However, it varies in terms of operations, therefore will AI-powered apparatus be used in offensive operations is still to be determined.
- The paradigms of warfare are changing. US Northern Command head Gen. Terrence O'Shaughnessy says the key to winning tomorrow's all-domain wars is predicting an adversary's actions hours and even days in advance. Synthesis of AI with increased situational awareness is eventually increasing the efficacy of the military, such as $1500 swarm drone using datalink and controlled by AI can enable 1000 such drones to perform simultaneously, in future will perform the same task as a $100 million jet. A simulated exercise, involving a human opponent to a unit mixed with robot, humans and drones reveals that they can do the same job that would have been done by a force 3 times their size. AI is lowering the cost of war overall, if there exists a moral cost of putting the responsibility and the trigger to a computer program will be the same or not is a different question to answer.

Recommendations on:
Legal Personhood of Artificial Intelligence

Research Area: Artificial Intelligence and Constitutionalism

Ananya Saraogi[1]

[1] Research Member, Indian Society of Artificial Intelligence and Law

- Sophia's citizenship had created a rift among the masses specially the software developers. The robot was not a form of AI and granting it citizenship had put forth several questions in the minds of the developers? Could autonomous systems be equalized to the citizens of a nation? Should there be a legislation that would regard an AI developed system as a legal entity?
- Artificial Intelligence has different branches including AGI and ASI. The amalgamation of the branches defines AI as a form which has the mental and physical capacity of or more than that of a human being. AI can be fiction; which cannot be touched, felt but its presence cannot be neglected.
- Jurisprudence has tried to entail rights or status to such fictitious aspects under the header of a legal person. Person has been defined as a being who is capable of sustaining rights and duties. Self-driving cars, chatbots, voice assistants are surely capable of performing the duties but for being entitled to their rights there is a requirement of these AI devices to be capable enough to decide their liabilities.
- A legal person can be solely held liable for the commission of his or her acts. Till now there was no computer program that could possess the capacity that could justify the question of legal personhood. Various legislations have been formulated for the regulation of autonomous systems but the details have been neglected. Assumptions of AI only possessing the ability to react based on the environment and not the human based emotional qualities have not been considered. This could be one of the elements for citizenship.
- Legal person need not be a citizen of the country, it does not need biological identity. A legal person need not possess the ethical or moral qualities; it could be imaginary or real in the eyes of law. accepting the fact that an AI device's functioning is not dependent on the commands but may vary on the basis of the actions in the environment. They have the capability to adapt and react to the stimulus; a scene beyond being regarded as a legal person. Could a legal entity be liable of a criminal act? Could the legal personhood act as a solution to the smart voice assistants who are rational in their thinking?
- Legal recognition of AI devices is essential in order to build the trust in storing the data among the users. Separate legislations are applicable for different AI built devices. Legal personhood being granted to all AI devices would cause chaos as not all AI devices are autonomous in nature and there are many which possess the human like qualities which include the decision skills.

- Decision making power of the AI has progressed over the last few years. It is no longer a pre-programmed system; the decisions are made based on the situations ahead. Some of the devices are completely aware of the existence of a grey area. There are many devices which are being deployed for serving justice; in such a case being a legal person could not be the apt status for these devices.

Recommendations on:

Artificial Intelligence in Corporate Transactions: AI, Automated Mergers & Acquisition and Corporate Ethics

Research Area: Artificial Intelligence and Corporate Governance

Stuti Modi[1]

[1] Research Member, Indian Society of Artificial Intelligence and Law

- The global market for Mergers and Acquisition in 2018 was worth $4 Trillion and amounted to 50,855 deals. Surprisingly, in 2019 despite of worries about potential downturn of global economy due to geo-political issues like Brexit and US-China Trade tensions, a 1% increase in deal value was witnessed, with only 2% downfall in deal count. The first half of 2019 witnessed strong mega-deal activity in the US, which was balanced by the slower second half of the year. Relevantly, the trend was opposite in Europe and Asia where the year started off slowly and the second half picked up. However, in 2020 with the anticipated Recession caused by Coronavirus it is essential to bear in mind that every downturn produces its own winners and losers which depends upon the strategies adopted, which differentiates them. The winners strategize to using scale and scope Merger and Acquisition and divest pro-actively in order to reshape their portfolios. This can be evidenced from the India M&A Report, 2019 which was published by Bain & Company in collaboration with Confederation of Indian Industry (CCI), where they reiterated that 70% of growth in 2018 was because of Distress Deals, enabled through the Corporate Insolvency Resolution Process under the IBC. Deals enlarging the sectors in which the business functions rather than helping it scale up its existing activities will lead Merger and Acquisition activities this year due to persistence of dynamics driving growth of these deals in the previous two years.

7.1 Expected M&A Trends in India, 2020

- It is expected that growth of M&A deals in the country will be favourable in the year due to the commendable regulatory regime introduced earlier by the government.
- Key reforms include reducing tax rates which in turn will incentivise manufacturing facilities either setting up or acquisition, thereby inviting direct or indirect foreign investment supplementing M&A deals. Further, expansion of M&A transactions is also expected out of CIRP Process under IBC and as entities contemplate expansion of its core/non-core vertical and horizontal business through buyouts, to maintain their competitiveness in the market. Moreover, divestment of group business lead by restructuring and reorganising in order to obliterate archaic ways of doing business

is another factor contributing to a positive and conclusive trend of M&A Transactions. Additionally, business initiatives facilitating foreign investments would not only contribute to growth of volume of M&A deals in the country but also value.

Imperative Requirement for AI in M&A.

- The year 2019, witnessed unprecedented regulatory scrutiny of M&A Deals. There is a tremendous rise in complexity, time and resources to surpass the regulatory hurdle. Consequently, resulting in costing more both in terms of cost and time. Further, highest deal failures can be traced back to poor due diligence that did not identified critical issues. The traditional approach of solely relying on Spreadsheet to analyse data is quickly becoming relic of the past. There has been a major shift towards a more dynamic, integrated and analytical process, tool and technique. This contemporary technique can be used to deliver what seemed impossible in the past, a combination of big picture insights and a microscopic level of detailed analysis, all in less time, effort and with more precision.

Adoption of AI still in pre-mature stage in Corporate Finance.

- AI has the potential of taking M&A Analytics to the next level, under which it is currently focusing on smart automation and making automation tolls and processes smarter and efficient. The efforts that were traditionally time-consuming, labour intensive and required human judgements is now being replaced with M&A Analytical platforms currently using AI and machine learning to analyse massive amount of data. Deloitte lead M&A platform called iDeal can not only make most of the work done with little or no human involvement but also learns from its mistakes when humans make correction, becoming more reliable, updated and accurate. Even in India, MnA Genome adopts AI as a tool to facilitate decision making at the due diligence stage and can also be used at the post-merger stage to align culture of both organisations.
- However, the actual deployment of AI is still at an early stage in Corporate Finance as compared to other professional services. One factor being complexity of large corporate transaction, which makes it difficult to replicate and standardize tasks that need human judgement, collaboration and experience. In M&A deals it is difficult to reduce to replicable process since each transaction has a specific nature. Activity being heavily focused on data in Corporate Financing, the issue is with the accuracy and reliability. Work is required to clean the data to use it for AI application. A massive shift will be seen when data will be cleaned at source, transferred and stored with accuracy. This will minimise the grey areas. For people who think they can work with nothing but clean data, it should also be borne in mind that it is wasteful waiting for perfect data since it is not always practicable or cost effective to clean it up. In most business context, data would be cleaned only when it mattered for reasons of cost, trust or safety.

Proposed Integrated use of Humans & AI.

- As the Discussion Paper on National Strategy for Artificial Intelligence by NITI Aayog has validly established, the deployment of AI in each sector is supposed to consider the incremental value the adoption of technology can provide to improve the pre-existing processes within each sector. The primary aim is to enhance the process for efficiency and effectivity rather than aspiring to be a tool to replace human decision-making in its entirety. This paper proposes an integrated human and machine-learning process in order to identify, classify, prioritize, organise and highlight document, which must be disclosed for business combination agreements for higher efficacy and speed and lower cost than humans alone can. The paper further suggests that an automated model, particularly Reflexive Random Indexing, can add appreciable value to the M&A due diligence process by identifying and indicating clearly related indirect connection.

7.2 Proposal of AI deployment in various stages of M&A Deals Process

AI in Deal Origination.

- For at least two decades, web-based match-making services have been around for buyers and sellers of small companies. For example, New-York based Axial Network, being a new generation online service provider, is using algorithms to recommend most relevant parties that the buyers and sellers can approach, by taking into account each buyer's and investor's real-time intent, along with strategic and financial interest on both sides of the deal. Further, Euan Cameron, UK AI lead at PwC, highlighted that AI could be used effectively to learn from past deals, by identifying success and failure factors and inform the preferred characteristics of future deals. An even more futuristic approach would be to analyse historical data by understanding actual outcome of deals and to link this knowledge to features of the target company.

AI in Company Valuation.

- Identifying comparable business and assets is a crucial area which will benefit from integration of appropriate automated analytical process backed and checked by skilled professionals.

AI in Negotiation.

- AI can also be successfully used in negotiation which is considered to be the most human part of the deal. Right data is required in order to help identify clauses which commonly cause issue. Additionally, historical data could be utilized to identify what the market standard is on certain terms.

AI in Due Diligence.

- Prolonged expensive hours are required in viewing documents for M&A market. The due diligence process could undoubtedly be largely automated, leading to faster and cheaper transactions which have a better risk management. Reflexive Random Indexing deploys an efficient, elegant solution for the challenge of collecting, classifying, organizing, prioritizing and highlighting the corporate documents in issue integrated with Human input on risk assessment.
- It is further recommended for the success of the model to make it more iterative, continually accommodating, objective and responsive. This is because the agreements are continuously revised during negotiation. Additionally, the model would highlight the most relevant words in each document enabling faster manual review. The software could use different colours for different queries so that the users can evaluate multiple queries simultaneously. The user could then easily label documents as responsive or not, giving the model an opportunity to improve continuously.

AI in Deal Completion.

- The highly technical process of deal completion which in itself involves negotiations, can also be simplified by using AI. Learning and insights could be gathered from hundreds and thousands of previous contracts. The inherent potential of machines over humans in this context should be judiciously used.

AI in Post-Transaction to Exit/Divestment.

- The analytical tool underpinning AI can be used for value creation activities that the business might not have identified before, which have an extensive reach across industries and value chains.

7.3 Recommendations for Ethical and Legal Consideration

- With the deployment of AI in M&A transactions, issues of privacy and security, liability and accountability, oversight, evaluation, transparency, redressal, lack of due process causing bias and discrimination also need redressal.
- The recommendations for the paper propose a rule-based system applied contextually in designing ethics, due process, fairness and transparency. Moreover, an Algorithmic Impact Assessment is recommended, whereby the onus lies on the authorities to deploy guidelines and procedures for evaluating the impact of AI-driven solutions. A combination of delegating controlled discretion to automated system and adoption of Constitutional Principles of proximity, proportionality and arbitrariness to assess the use of AI in governance should be undertaken. An appropriate and contextualized process needs to be developed by the government, when decision making is being carried out by AI along with ensuring transparency regarding the factors undertaken for such decision-making. Further, Public Private Partnership requires a cohesive and uniform framework for regulating the partnership which is entered between

government and private sector. There is an imperative need for establishment of adequate Redressal Mechanism, which would foster accountability and would be accessible to all stakeholders. Interdisciplinary approach for furtherance of AI, which is attained by integration of technological progress along with economic, political, demographic, anthropological and legal aspects which account for fairness and due process. Additionally, the technology benefits must reach lowest common denomination, adhere to international obligations, Sustainable Development Goals and guarantee socio-economic rights. AI should be deployed in such a manner that the existing domestic and international human right standards along with commitment to the environment is honoured.

7.4 Conclusion

- Conclusively, the deployment of AI in carrying out analytics of M&A Deals would surely induce some challenges. However, not only such problems can be fixed but the merits of such adoption outweigh the demerits of it. Hence, the use of AI in M&A Transactions remains inevitable in the future.

Recommendations on: Artificial Intelligence and Privacy

Research Area: Artificial Intelligence and Constitutionalism

Nayan Grover & Vaishnavi Venkatesan[1]

[1] Research Members, Indian Society of Artificial Intelligence and Law

7.1 Introduction

- In today’s world, Artificial Intelligence is at the forefront of technological development. From merely texts in pages of a science fiction book to authentic existence, Artificial Intelligence has come a long way. Things that could only be envisioned earlier have now become a staunch reality. Some perceive it as a threat while several apprehend it as a tool for social good however irrespective of the perception, it is an indisputable reality of today’s world.
- Despite the plethora of information surrounding AI and envisioning its implementation for societal good, it raises numerous concerns. A highly debated issue is that of privacy considerations. Emergence of sophisticated AI in its multi-faceted domains, which are majorly data driven, have exacerbated privacy concerns. In this information era, privacy hinges on our ability to control how our data is being stored, modified, and exchanged between different parties.
- The following are recommendations for steps to be taken in order to ensure better privacy for a human being in this AI driven era. A part of recommendations provided are for improving certain general areas of the data protection regime so that when they interact with Artificial Intelligence, better privacy is ensured. While other solutions are specific to the interaction of Artificial Intelligence with consumer data.

7.2 Recommendations

- India presently does not have a data protection law however the Personal Data Protection Bill, 2019 which envisages a comprehensive policy on data protection is in development and is pending approval, which was the backdrop of the Justice K.S.Puttaswamy (Retd) vs Union Of India judgement. India needs to adopt a comprehensive framework for the regulation of data which suits the best interests of the country whilst dealing with omnipresent problems that plague the current landscape of data privacy in India. It needs to provide rights to individuals with stringent measures prescribed in cases of contravention of the same.
- It is imperative that the data protection law, which is to develop into the law of the land, should be free of bias. In its current form, the bill provides unrestricted access

to government agencies for matters of 'nation concern' or in the interest of the sovereignty and integrity of India. These terms are vague and leave room for ambiguity to kick in thus paving way for misuse of the provisions and defeating the very purpose of the act. Situations wherein the government can bypass such checks and balances should be dealt with exhaustively. It is imperative that more accountability and transparency be attributed to Governmental organizations/ agencies while dealing with the subject matter.

- It is proposed that India needs a Central Data regulatory authority which will act as the sole body handling data, leading to an increase in centralization and transparency whilst dealing with sensitive personal information. Instead of information being scattered across multi-faceted domains, it would pass through a designated authority which shall be the fiduciary holder of this data. The concept of data protection officers as listed in the GDPR can also be implemented in India by molding it as per requirements wherein the data protection officer would be responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with the country's policies and framework.

Keeping It Simple.

- Privacy Policies drafted by companies should be in plain simple language. The privacy policy is drafted for consumers, who don't prefer reading technical jargons or legalese, so use of them should be avoided as much as possible. The Privacy policies are lengthy in the first place and a further addition of Technical Jargon and Legalese makes it even more difficult for consumers to read and comprehend it. A study by New York Times included analyzing the readability of privacy policies of different companies by using a Lexile test developed by the education company Metametrics. The test measures a text's complexity based on factors like sentence length and the difficulty of vocabulary. They analysed 150 privacy policies and except two or three all others were found to be much less readable and more complex than the college study texts. This rings alarm bells and makes consumers more vulnerable to a privacy breach since the privacy policy to which they consented was not completely understood by them. In India where most of the population with access to internet is not digitally literate or is at a premature stage of understanding these nuances, this becomes a much huge problem. Consumers should not need an understanding of complex methodologies and processes involved in data collection in order to understand where their data is being used. And So, it should be mandated by the Data Protection Law in India that companies should have their privacy policies in plain and simple language which could be evaluated by some method or tool like the one involved in the study done by The New York Times.

Choosing Rights Over Consent.

- Until now data protection frameworks have had a consent-based approach i.e. where companies could collect and use data of consumers in any way after acquiring their consent on a privacy policy through click wrap. But in today's age when data terminologies are so complex and as mentioned above the privacy policies are not easily comprehensible for a common consumer. Thus, it is suggested that while framing data protection laws a Rights based approach should be followed where certain guidelines are laid out by law as to what extent and manner the data of a consumer, although obtained with consent, can be used. Such laws should limit the use and collection of data in a manner to protect the violation of data rights of consumers. Breaking of such laws should lead to penalisation of the corporation doing so. This would make corporations and organizations handling consumer data more accountable as to their usage of that data. Especially in a country like India where a larger part of the population which has access to technology is not much digitally literate and is trying to learn little by little every day. These types of consumers are most vulnerable to violation of Data and Privacy rights and so a rights-based approach becomes more necessary for a country like India.

Opt-in rather than Opt-out.

- To discover a consumer's consent status, there exists two systems for data collection – Opt-in and Opt-out. In an Opt-in system for data collection, data collection is turned off by default and the consumer has to expressly give his consent in order to start data collection whereas in an Opt-Out system the consent is already presumed to be given by default and the consumer has to retract it if he wants the data collection to stop. To ensure that the consent given by consumers is closer to real consent, we need to ensure that the companies follow a strict Opt-in policy of Data Collection. Although General Data Protection regulation imposed a strict Opt-In system, the issue is still heavily debated. The pro Opt-out system group argues the following three major concerns – (1) It is that the consumers are likely to prefer the initial option set for them and it is highly unlikely that they'll change the option to allow their data being collected no matter how convenient and clear it is made. It is based on the presumption of general preference of status quo by consumers. (2) It is stated that opt-in requirements can pose significant transaction costs to data collectors previously uninhibited by consent gates. An opt-in regime imposes more pronounced legal costs, technology process management, and business operations costs than does a typical opt-out regime. (3) It degrades the user experience by introducing unwanted disruptions like asking for consent prior to the main content being introduced which annoys the consumer and makes them prone to leave. Now all these points are not well established. The world we live in where our data can be used in numerous adverse ways, it becomes really important that the consumers are well informed about the data collection and they agree to it prior to it being in effect. The above-mentioned concerns can be well handled by introducing a much simpler privacy policy as mentioned earlier and it is much more likely consumers won't mind a little disruption if they know that it is for their own safety and security. The current proposed method for Indian Data collection Regime is also Opt-In for the companies except when it comes to the government which is also a big concern.

Opt-in and AI.

- This Opt-in system might be followed in the usual data collection by websites, but it is not even remotely followed when it comes to data collection by Artificial Intelligence. Data collection by Artificial Intelligence at a lot of points is without consent and even unflagged. And as stated earlier that how much more deeply our data can be used with the help of an AI it becomes even more crucial. The personalised AI powered medical advice portals, the online retail sites and the AI Traffic Cameras don't warn us and neither ask for our consent before analysing and storing our data beyond the scope of what we provide them for.

Proper Cautions Necessary.

- There must be proper warning at all places wherever there is a chance that the consumer's data might be collected and stored by an Artificial Intelligence enabled system and when it is collected for synthesis by an AI. Now it is even more important for us to learn when an AI enabled system is collecting our data due to its much larger ability of doing so. And at many places it does so without warnings like when google maps use location information of hundreds of users to warn about traffic to its other users, license plates being captured by plate readers, driving speeds and car information captured by AI traffic cameras, Tesla self-driving car systems storing every detail of our drive, our face data being stored by airport security face recognition system etc. Now gathering all this information is necessary for AI to provide better services to us but a caveat every time it collects data can be provided so that we can ensure that it is only collected to provide better services to us and not for any other interests. In a world filled with Artificial Intelligence all around us there need to be red flags everywhere where our data is being collected by them.
- To be at the forefront of the AI revolution, is imperative to take proactive steps since the dangers and problems associated with AI are not yet completely known. Consequently, it is vital to have a two-layered protection model: one- technological regulators; and two- laws to control AI actions as well as for accountability of errors. Technological regulators include introducing a multi-layered security and defense software to protect data and in turn business. Layered security strategies are reactions to today's cyber threat landscape. Rather than simply waiting for attacks to hit endpoints, layered security takes a holistic view of cyber defense, accounting for the multitude of vectors by which modern malware is delivered. Apart from this, laws which protect the rights of consumers and ensure transparency and accountability along with these technological regulators will be an advantage to ensure privacy concerts pertaining to AI.

Right to be Absolutely Informed.

- There should be a clear declaration made to the consumers with regards to third parties using their personal data. The law should mandate it for companies to disclose the list of third-party organizations to consumers who will be accessing and using their data and also clearly state in the disclosure as to what part of the consumer data is provided to which organization for what purpose. Another important part of being absolutely informed should be the Right for individuals to receive the reasoning underlying any automated processing of their data, and the consequences of such reasoning for their rights and interests.

Machines Learning Safely.

- Machine Learning Algorithms are often trained to predict outcomes based on certain sets of data. These outcomes can be related to a mathematical issue or social issue etc. In order to achieve high, reliable levels of accuracy in prediction, these systems rely on large sets of data to learn from. These data set often involve personal and sensitive information of people. The issue of data privacy is amplified with machine learning. This data is forever stored with machine learning systems. These systems are even capable of re-identifying personalized data based on only minimal information. There is also a lack of transparency in how this personal data might be processed. In order to meet the needs of the future it is very crucial to train these machine learning systems but keeping privacy protection in mind is also necessary. So certain guidelines can be made mandating certain practices to be followed while training machine learning which protect the privacy of the people whose data is being used in the training process. These practices could involve – Federated Learning, Differential Privacy, Homomorphic encryption etc as per the recommendations of the experts in the field
- Transparency and accountability also form an important part of the training process because in numerous cases there is a manifestation of unwanted bias which is reproduced via people building it or through biased data which is fed to train the AI and Machine Learning algorithms. In such a scenario, transparency and accountability are two major pillars which will prevent the structure of AI from being corrupted and ensure it remains free of bias.

Right to Erasure.

- Right to Erasure enables any data principal to have his personal data deleted from all databases on his request. It is an essential part of European Union’s General Data Protection Regulations. This right ensures that a consent is valid only till it is an active consent. If once a consent was given for an information to be collected, it does not mean that the information shall be withheld for lifetime. This also provides a person an opportunity to get any false information about him, present on the internet, to be removed permanently. It is also famously known as “Right to be Forgotten” worldwide, which is different from the Right to be Forgotten envisaged in Indian Data Protection Law that only allows users to stop their data being disclosed any further on their request. Right to Erasure is a big step towards strengthening a person’s privacy. Although it is a qualified right, but still a valid request of Right to Erasure goes a long way in protecting a Person’s previously collected and retained from being exploited any further.

Can AI forget?

- Right to Erasure becomes complicated when the data has been fed to Artificial Intelligence and Machine Learning systems. The first issue this raises is of how to reclaim the data and its influence on the resulting output. Generally speaking, AI cannot be taught how to “forget” something the way a human can. Technical experts do suggest a solution i.e. that if the key that allows AI to access a particular data is removed then the AI won’t be able to access that particular data and thus Right to Erasure would be met. Now coming to the second and much bigger concern i.e. the impact on the performance of AI and Machine Learning algorithms of the data being deleted. Although one person’s data being deleted wouldn’t have much effect but if thousands of people exercise their Right to Erasure then it could lead to a mess in AI’s performance. And so, it is recommended that the Right to Erasure be never made an absolute right so that if the data is crucial for the performance of AI, the right can be denied.

Governing Privacy in Time of Crisis.

- There is a need for certain legislative regulations in the data protection law that can govern the realm of privacy in crisis situations such as occurrence of war or outbreak of a pandemic. These regulations should mainly focus on regulating the actions of government during the crises. It is often seen that in the time of crises the government takes an undue advantage and under the garb of controlling the situation, it breaches the privacy of its citizens to a far extent. For example currently in India, the name of controlling the corona virus outbreak the government has rigorously increased surveillance over the general population. They are using drones with facial recognition systems in the background in order to track and trace citizens. The Aarogya Setu app introduced by the government and now being imposed on citizens through various ways has a flawed privacy policy. This app collects highly sensitive data related to health and whereabouts of the citizen and there is no clear mention of the purpose of usage in the privacy policy and also there are no clauses in the privacy policy which limit the retention of data until a certain period of time. It is obvious that the government needs to be provided a bit of loose hand in such situations as health and life always trump over privacy but that loose hand should have some limits. Thus, the extended lineage provided to the government as to violation of and restrictions on the government to ensure the protection of privacy of the citizens in the time of a crisis should be clearly defined beforehand in the data protection legislation of the country.
- Awareness is one of the most important tools to combat AI considerations and privacy aspects. India’s low literacy levels acts as a major barrier to the common people understanding privacy laws and resolving complexities, conducting, and inculcating public consultation goes a long way. If people are aware of the rights that vested in them, data can be circulated and regulated in a controlled manner where the individual is provided with ‘real’ options to regulate data in the manner they feel right, along the lines of GDPR.

7.3 Conclusions

- AI is ubiquitous in our everyday lives. It is the new ‘normal’ and is making a difference in numerous fields. It is defining our lives in new innovative ways every day. Its impact on society cannot be negated in any manner whatsoever. There exist numerous AI's that aid essential areas such as law enforcement to provide novel solutions to omnipresent problems, gradually annihilating the gap between already diminishing human and AI functions, amongst performing other functions for the overall betterment of society. However, with increase in involvement of AI in our lives, increases the exposure of our information to this world which leads to increase in threat to our privacy. The matter pertaining to privacy is a subject of great concern which needs to be addressed appropriately by way of a robust legislative framework covering all aspects mentioned above.

Recommendations on: Machine Learning and Privacy Mechanisms in India

Research Area: Artificial Intelligence and Constitutionalism

Sameer Samal[1]

[1] Research Member, Indian Society of Artificial Intelligence and Law

- Democratic establishments throughout the world have incorporated privacy, including informational and data privacy, as an inviolable facet of the right to a dignified life. Thus, to safeguard the said right, it is imperative to establish a legal framework to protect personal data throughout all industries. With the advent of advance technologies, such as Machine Learning, the necessity to protect personal data has increased significantly. In furtherance of the same objective, the paper analyses involvement of personal data at various stages of Machine Learning and recommends protective measures. Although central legislation is required to govern data privacy in general, it is also imperative that specific industries implement data privacy policy measures targeting the protection of data generated and collected by the industry. Therefore, a policy framework consisting of central legislation and industry-specific policy is recommended.
- The following policy measures are recommended in the central legislation:
  - Granting absolute data ownership to data principals for all categories of personal data.
  - Enforcing liability over Machine Learning developers by establishing data principal-data fiduciary relationship.
- The following policy measures are recommended in industry-specific policy measures:
  - Enforcing compulsory data anonymization in datasets.
  - Mandatory usage of specific learning methods for certain industries.
  - Regulate data purchase from private entities.
  - Sectoral data localisation obligations.

Data Ownership.

- Individuals to be granted property rights overall categories of their personal data. Majority of the industries do not provide property rights over personal data to individuals. However, certain industries, such as the healthcare industry, provide partial ownership. The data in medical records is owned by the patient but the medium of transmission and storage is owned by the healthcare provider. In such situations, although the data is owned by the data principal, he/she does not have any control over the medium of storage and transmission. At this juncture, regardless of central legislation that grants property rights over personal data, the intervention of industry-specific policy measure to ensure uniform rules for collection, transmission, dissemination and storage is necessary. Granting property rights over personal data to individuals would ensure a strict consent-based usage of such data as individuals will exercise absolute control over the generation, transmission and secondary usage of their personal data.

Compulsory Anonymization of Personal Data.

- Anonymization methods such as K-anonymity, L-diversity and T-closeness are commonly used to mask or remove personally identifiable information and sensitive column data from ML training datasets. These anonymization techniques are currently voluntary in practice and India does not have any policy measure to enforce such safeguard measures. Industries such as Agriculture do not generate personal data and thus require minimal data protection. However, Financial and Healthcare industry generates sensitive and critical personal data, and thus require stringent anonymization measures. The Government of India also offers certain open-access datasets containing data from various Ministries to enable innovation and development in India. Therefore, even if explicit consent is obtained from the data principal, it is essential for the aforementioned industry-specific data governance policy to enforce such anonymization techniques before personal data is used in ML training datasets.

Mandatory usage of specific learning methods for certain industries.

- The Draft Personal Data Protection Bill, 2019 has categorized personal data and has proposed general regulatory measures for the specific category. The proposed regulatory provisions are indeed promising but will fail to achieve its objectives if data is used for secondary purposes, such as Machine Learning training datasets. Therefore, specific learning methods have to be introduced for certain industries. Machine Learning algorithms' training on clinical data for Healthcare development should be mandatorily performed using 'Federated Learning' likewise training on financial data for Investment and Banking development should be mandatorily performed using 'Shared Machine Learning'. The aforementioned learning technologies, although voluntary, have been already implemented in certain overseas organisations. The industry-specific data regulatory policies for the Healthcare Industry and Investment and Banking industry should impose the mandatory usage of such training methods.

Regulate Dataset Purchase from Private Sector:.

- The Government of India offers certain open-access datasets containing data from various Ministries to enable innovation and development in India. However, it does not consist of robust and comprehensive datasets across various sectors and fields, thereby creating a shortage of quality intelligent data. The quality of the dataset affects the performance accuracy of the Machine Learning program. Considering the lack of any legislative policy for data protection in India, majority of the data is owned and controlled by the private sector, and thus Machine Learning developers turn to private sector industries for datasets. However, due to the high costs of such private-sector datasets, small-scale innovators and startups face a serious obstacle. Therefore, a regulatory framework has to be established that regulates the pricing and quality of the datasets to ensure a fairground for innovation in India for both large-scale innovators and startups.

Sectoral Data Localisation Obligations.

- Considering the multitude of opportunities emerging from Machine Learning technology, the correct rationale for a developing country like India would be to analyse data localisation measures. Industry-specific data localisation measures for industries that generate sensitive or crucial personal data would ensure local storage of such data, increased accessibility to government institutions and growth in innovation. Local storage of data would provide the government with better access and control over citizen's personal data. The rate of accessibility of data for quality machine learning datasets will likewise improve. Industry-specific data localisation obligations are more favourable than absolute data localisation measures overall industries as an absolute measure would cause a negative economic impact.

Recommendations on:

Artificial Intelligence and Intellectual Property: Collateral Parallelism

Research Area: Artificial Intelligence and Intellectual Property Law

Vasudha Tewari[1]

[1] Research Member, Indian Society of Artificial Intelligence and Law

- AI is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. Computer systems began to mimic our perception and cognitive ability, our ability to create; these abilities are those for whose guidance and protection the laws and the law makers were primarily made. AI machines have several such qualities that make them stand equal to human beings.
- AI can gather data and feedback and process those to improve their ability and create new and magnificent things that human can or even cannot without almost any human interference. These machines have the ability to learn and to take decisions based on that. Now the question which comes into light is when an AI system creates something on its own without any human interference will that work be made a patent? Will that system get the credit for that innovation or the owner of that system will be granted patenting right? Or the question which actually is getting discussed is whether such work should be granted patenting rights, like granted in the case of human being?
- Current patent laws treat AI software inventions essentially as logical algorithms implemented on the computer. On inventorship, patent law states that someone (usually a natural person) who merely applies the logic to make something workable cannot be an inventor. So far machines were 'that someone', hence they were not a possible inventor under the law
- According to WIPO, Intellectual Property is – to the unique, value adding creations of the Human intellect that results from human ingenuity, creativity and inventiveness. And what IP Laws do is to confer property like rights on these inventions or creativity. Simply speaking by assigning property rights on the product of our intellect laws give us control or exclusivity over that particular property or product. IPR can be said to be working as the root of the innovations.
- The office of technological assessment in 1986 said that artificial intelligence should be considered legitimate co-authors. Critics has said that machine follow a routine as set by humans thus it cannot be considered as something worthy of patenting. It

was suggested that copyright production should not be granted unless granted to the creator, i.e., human beings on behalf. In the matter of patentability the three important criteria to be kept in mind are novelty, inventive step and industrial use. But in the case of AI it is considered that novelty is not present, as some prior data has to be entered in the device or machine to make it work accordingly. A machine cannot develop the data in its own, thus it cannot be totally different of the prior art. Many inventions produced by AI are generally driven by Deep Neural Networks (DNN) and are heuristic in their behaviour. In such cases, we can focus on the end-result obtained from the process and not on the process itself. If the end-result meets the criteria set forth as 'sufficient to imbue a human or natural person' with an inventor status, then consequently the machine (or AI system) could also be imbued with the same status.

- Currently we have AI created music and art work. Example of such is e-David who is a robot and has done commendable work in the art field. It creates the portraits which never primarily existed by analysing and observing the features like we human do. University of London Press Vs. University Tutorial Press said "the word original does not in this connection mean that the work must be expression of original or inventive thought. But that the work must not be copied from another work but should originate from the author."
- In US to qualify as a work of authorship a work must be created by a human being. In the case of Naruto Vs. Slater where Naruto a monkey took some photographs, the US Court said that being an animal, i.e. non-human, he does not have standing in the court and cannot sue for copyright infringement. In 2010 US Supreme Court denied patenting to the programs because what they perform is mechanical rather than inventive. Similarly in Nigeria AI systems are said to lack legal personality and cannot be authors. Now in India there are no guidelines for AI related inventions but computer related work has been discussed and appreciated by making laws for the same timely.
- UK has expanded the scope of copyright protected work to expressly include the computer-generated work. The author of such computer generated work according to section 178 of UK Copyrights, Designs and Patent Act, is deemed to be the person by whom necessary arrangements for the creation of the work are undertaken.
- Somewhat same idea has been perceived in Europe where European Patent Office has laid the guidelines where list of exclusions has been made. One of the ingredients of that list is Mathematical methods and programmes by computers. EPO has also made guidelines specifically for AI related inventions. It clearly states that when an AI classification method serves a technical purpose, the steps to generate the training set and train the classifier may also contribute to the technical character of the invention, if its support achieves the technical purpose

Existence of AI should be recognised and such organisations should be made to deal solely with the recognition of AI and the laws to be made for them. Detailed and logical guidelines for patenting and copyright of the products of AI should be made at international level and implemented uniformly. We must acknowledge that AI systems demand a reconsideration of the extant IP laws. Intelligent IP should managed be in various ways like Data Privacy where high quality and accurate data can be accessed, by enabling the IP systems and tools with AI-based solutions , by empowering people to realize the benefit of AI in the IP domain an etc. IP management can greatly benefit in using AI during patent search and prosecution phase. Similarly, there could be more AI benefits that are not yet realised in IP. But what required for that to achieve is that as there is no sustainability currently in the field several steps should be considered for that. There should be uniformity across jurisdictions, the system where a work is protected by laws in UK and is not in Nigeria is vague and should be made more precise. A multi-trading platform needs to agree on a position. IP rights for AI invention and creativity should be considered side by side criminal and civil liability for such rights. We should also consider that giving copyrights or authorship of an AI generated work to a human will lead to those inventions getting exploited by those who haven't even created them. As the upcoming lawyers it becomes our duty to adapt such great changes and change the law according to the needs of this generation. The speciality of the lawyers is that we acknowledge past and consider future while deciding the present. While the scope of IP management automation and using AI tools is colossal, it is just a matter of time when IP management will become fully automated and self-driven.

Indian Strategy for AI & Law, 2020

Indian Society of Artificial Intelligence & Law, 2020.
Published on May 19, 2020