INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 4

2020

Emergence of AI and its implication towards data privacy: From Indian legal perspective

D. MAJUMDAR [1] AND H.K. CHATTOPADHYAY[2]

ABSTRACT

Artificial Intelligence (AI) is a concept that the intelligence should be artificially exhibited by computer systems which were previously unique to mankind. These AI algorithms can analyze and solve different complex problems without human assistance. Thus, analysis of data including personal data by AI and to reach an intelligent decision has provoked various sectors to use these AI algorithms. Thus, use of AI has benefited considerably different sectors. However, such easy access to the personal data by AI has brought in ethical and legal dilemmas for ensuring logical balance between use of personal data by AI and fundamental privacy protection rights of personal data. These dilemmas have become instrumental for rapid advancement of technology and its ever-increasing use in the society through AI algorithms. This modern technology has become able to easily access and analyze Personally Identifiable Information (PII) which has made different organizations updated to achieve success. This has also lead to question if the privacy of personal data is at stake, especially when Supreme Court of India in a recent judgement (Puttaswamy and Anr v Union of India & Ors) has held that right to privacy is a fundamental right under the constitution. The apex court further observed inter alia that there is a need of technology-neutral data protection law to control the growing use of AI in India under the legal discipline. In this background, this paper has tried to analyze as to how applications of AI can be guarded not to endanger data privacy from legal perspective under different platforms, whether the personal data protection bill is adequate to combat the misuse of AI in India, what are the legal issues to put a balance between use of AI and data privacy protection.

Keywords: *Artificial Intelligence, Data, India, Law, Privacy*

I. INTRODUCTION

The concept of Artificial Intelligence (AI) is not new. Even during 1950s, this AI was considered as an effective technology as people even of those days possessed high hopes of

[1]Author is the Head of the Institute at BGHS, Education Department. PhD from North Bengal University, West Bengal.
[2] Author is a Legal Consultant, Calcutta University, Kolkata, West Bengal, India.

 [ISSN 2581-5369]

success regarding AI. However, initially such high hopes of success of AI was effectively not achieved but with time, people have witnessed considerable success of AI (Roberts, 2014). AI is referred to as systems which are versatile like humans especially when we think of problem solving (Lawless and Sofge, 2017). However, it took several decades to reach this position. AI is considered as a computer-based technology that can solve various problems under varied situations in an accurate, cost effective and easy manner without human interference[3]. These were previously thought to be unique to mankind (Barrat, 2013, Bostrom, 2016). Most of the applications of AI need huge volume of date including personal data. From these data, AI technology learns something and can make intelligent and accurate decisions without human intervention[4] (Autor et al., 2003) Owing to its easy, accurate and cost effective capabilities for decision making without help of humans, this has found a high position on the agenda of most of the sectors. These sectors cannot perceive to sail on minus the help of AI. This ever-increasing use of AI in different sectors under multifarious circumstances is apprehended to face a range of ethical and legal dilemmas while searching for an effective balance between social advances covering use of AI and fundamental rights for protection of privacy of data (Brown and Sandholm, 2018, Chatterjee et al., 2019). It is conceived as a high time to realise the situations as to how privacy of data protection is affected by the rapid and effective development of applications of AI (Moravcik et al., 2017). With this belief, the Government of India has already brought a bill in the parliament for introduction of an enactment to protect data (Ghosh 2019, 2020; Chatterjee 2020).

This has become essential because rapid development of AI has substantially made some effective and major advances. Its potentiality has become promising and has interfered in the developmental activities of the society. It helps to protect environment, it has helped to improve efficiency of public and private sectors effectively (Solaiman, 2016, Chatterjee et al., 2018), it has been able to make the society safer and even AI has helped to cure cancer. Such huge use and utility of AI in all sectors of our public life have created a possibility of unknowingly misuse personal data at the cost of privacy.

The date protection regulations are expected to appropriately strengthen protection of private data. The organizations dealing with big data are expected to process personal data in a more cautious way in accordance with the data protection regulations. The requirements for enforcing transparency will be then more stringent (Chatterjee et al., 2011). In this background, it is important to understand status of AI in Indian Jurisprudence. This article

[3] "Robots for Business" written by Jsabelle Boucq. This will be available at http: //www.Atelier-us.com/ emergingtechnologies/article/robots-for-business. (Last accessed on December 27, 2018.)
[4] Artificial Intelligence and Intelligent Systems[3] (2005), Oxford University. Writter is N.P. Padhy.

 [ISSN 2581-5369]

has taken a holistic attempt to emphasize to analyse the legal implications for keeping the misuse of AI in check so that privacy of data can be protected (Bhattacharya et al., 2020).

II. INTRODUCTION OF AI AND ITS LEGAL IMPLICATIONS

AI has considerable impacts on all spheres of our lives. It has effective and major implications for professionals using this modern technology, for legal practitioners dealing with the effect of use of AI and its legal implications, for technocrats frequently using AI to fetch accurate decisions and even for the citizens at large (Chatterjee, 2015). In the present scenario, all the stakeholders including different organizations and governments have closely come together to sort out the growing questions covering ethics, global governance and business processes concerning to the applications of AI in their respective working fields. This has needed to manoeuvre imminent alteration or modification in existing legal framework to combat the problems of protection of personal data while applying AI to analyse those. The legal dilemmas developed concerning rise of ubiquitous applications of AI are needed to be reconciled by effectively bridging the unwanted gap between law and technology (Vladeck, 2014, Ghosh et al., 2020, Chatterjee, 2020).

(A) Understanding AI

Before we penetrate to ferret the essentialities and potential of AI, it is pertinent to step back to realise and conceptualize what is meant by AI. Though interpretation of 'Artificial' is not a tough work, the conception of 'intelligence' in the generic term, especially, befitting in the context of AI is bit complex (Kritzer, 2015, Kar et al., 2019) since intelligence is considered artificial to that extent as it emerges from human-created systems. This intelligence[3] is not completely artificial as it does not possess consciousness. This 'intelligence' can be considered as hypothetical intelligence and we can call it spontaneous intelligence (SI).

This intelligence is considered to emerge from a conception in the context of seeking some form of social acceptance and recognition as a legal person (Chopra and White, 2004; Hallevy, 2010, Ghosh et al., 2019). Many experts have taken holistic attempts to define AI, but studies reveal that there exist different opinions relating to define AI. On the other hand, many experts argue that ascribing a coincised definition of AI might have effect to limit the amplitude of AI-applicability (Chace, 2015, Chen, 2018, Chatterjee et al., 2019). It may be considered as a decision-making software working independently to come to a decision without slightest human interference. However, so far as regulatory purposes are concerned, for understanding AI, it should be considered by way of analysing its applications in the practical fields.

 [ISSN 2581-5369]

(B) Different AI Platforms

Different applications of AI have captivated attention from the major technological players in the World. They are Microsoft, IBM, Google, Facebook, Amazon to name a few. These technological players are using different AI platforms. These are shown in a tabular form in Table 1.

Table 1: Different AI Platforms

Platform	Description
Microsoft	Microsoft Chatbot (Xiaoice); Cortana Intelligence Suite (Knowledge, Speech, Vision, Language and different search APIs).
IBM	Cognitive Solutions Platforms: Innumerable offerings like machine learning, cognitive computation technique, natural processing of language, predictive APIs, deep learning.
Amazon	Techniques associated with creation of models and to find patterns towards data for making new predictions covering new data (Amazon Machine Learning Services).
Facebook	Facebook AI Laboratory – Research documents publishing reports concerning to progress in collaborative effort, engagement in workshops and conferences, open source software – different AI modules.
Google	Cloud Machine learning services in different forms (Deep Mind).
Infosys	An AI platform that aggregates organizational data from processes, people, legacy systems for analysis and thereafter automates recurrent IT and business processes, attempts to solve customer problems. These require creativity, imagination and profound passion.
Rainbird Technologies	Decision making platform which automatically takes decision. It is an inference-oriented automated engine to be utilised in specialized industries like Banking, Financial, Law and so on.

III. Present Personal Data Protection Scenario in India

India is now advancing towards use of digital economy. Use of AI in different sectors has become ubiquitous. Consequently, use of information of different types has automatically

brought in great concern over cyber security, data protection and data privacy. This concern has gained special importance and momentum in view of the recent Supreme Court verdict to the effect that privacy is a fundamental right. This has facilitated the need of providing a meaningful, implementable, comprehensive legal framework to combat the concern for data protection.

(A) Scope and Legal Implication

1. Applicability

Borderless character of AI has ignited several jurisdictional issues. Processing of data might occur across various jurisdictions where the state ordinarily might not have jurisdiction to exercise. The data protection framework should address this issue as this extra territorial applicability and issue of jurisdiction might pose great concern. The legal framework must have its applicability to any entity that deals with processing of personal data of Indians regardless of the fact as to where they are located (Garner, 2005).

2. Persons whose privacy to be safeguarded

Data privacy law must possess a data subject, that is, a person. The aim of the legal framework is to provide a full proof safeguard to the personal data of the persons. Law provides two types of persons – natural person and juristic person. Natural person is a living person whereas juristic person is not a living person but an entity that has been given legal personality by law, as for example, a company. Data protection framework would apply to a natural person and not to a juristic person. Financial information of a company (like PAN) is a data of juristic person. It is excluded from the data protection framework. (Chopra and White, 2011).

3. Personal Data

Personal data is that data from which an individual can be identified or can be reasonably identifiable. The affairs of identification may be direct or may be indirect. It includes any kind of personal information including assessment or opinion regardless of the accuracy of the data. The legal framework is required to protect personal data.

4. Entity, Processing and Accountability

It is a fact that both public and private entities by the help of automated devices (AI) have started to analyse personal data of the data subject. While analysing, both public and private entities are required to ensure protection of personal data appropriately. The data protection framework is expected to ensure this. The private and public entities would process the data

 [ISSN 2581-5369]

with the help of AI (Kassaro and Norton, 2010). This processing includes collection, use of disclosure. At all stages, the processing activities must be transparent so that data protection is aptly ensured. The legal framework should cover this point to avoid the scope of misuse of AI application.

While processing the data by any entity with the help of AI, the legal framework should include modus operandi to identify the party accountable for compliance so that protection of data privacy is not at stake. Both the data processor and data controller are scheduled to be accountable to ensure protection of personal data (Kraakman et al., 2017) being analysed by AI algorithm.

5. Relaxation in processing and issue of consent

There are many legally accepted and recognized grounds concerning to processing of personal data. (Leenes and Lucivero, 2014). These are needed. The framework should recognize those. The framework is supposed to recognize and allow processing of personal data legally on the grounds of legitimate interest, public interest, major interest and other residuary grounds of interest. However, except on these grounds, if processing of personal data is needed by the help of AI or otherwise (Teubner, 2006), the consent of the data subjects is essential. The legal framework for combating misuse of data by AI algorithm must focus sharp attention on these points. Legal circumference confining data protection activities is supposed not to be unreasonably street.

6. Dealing of Personal Data of Children

In India children are gradually becoming technologically savvy. This has invited high vulnerabilities for being attacked. Organizations using children data should be cautious on some of the issues like verification of age of the data subject and so on. Prior to processing personal data of children, parental consent is needed. Proper security measures are to be taken while, with the help of modern technology like AI, the personal data of children are being processed (Lee and George, 2008).

There are other important and salient points like jurisdictional issues, issues connected with limitations to control AI applications and so on. These are scheduled to be kept in mind to provide legal framework to combat the issue of protection of personal data while dealing with through modern technology like AI.

IV. STATUS OF AI UNDER THE LAW EXISTING IN INDIA

No doubt that the Constitution of India is appropriately considered as the principal legal

 [ISSN 2581-5369]

framework which covers the obligations and rights of persons in ensuring the privacy of personal data, especially in view of the Apex Court verdict that privacy is a fundamental right[5].

However, ironically, the Indian Courts have not yet explicitly adjudicated the status of AI legally. Had it been clearly adjudicated, it would have taken an effective measure to clear up the growing debate and dilemma concerning the legal applicability to AI algorithms (Kurki and Pietrzykowski, 2017).

Since the applications of AI have become universal in India, since growth and development of this system are instrumental in improving technological health of India, since recognition of AI has been accepted for nation's growth as a whole; the Ministry of Industry and Commerce, Government of India has formed a task force for exploring the possibilities to leverage AI ensuring overall development across multifarious sectors. It has been formed in August 2017.

The task force comprises of 18 members including researchers, experts, industry leaders, government bodies, academics and other Government Departments. The task force titled as "Task force on AI for India's Economic Transformation" is chaired by Prof Dr. V. Kamakoti (a professor of IIT, Madras). This task force has already published its report[6] (August 2017) with recommendations including actions required for next step for formation of a comprehensive, executable policy concerning applications of AI in India. The task force has submitted its report to the Ministry of Commerce, Government of India.

(A) The key takeaways

a) From the perspective of applications of AI algorithms, ten specific sectors have been identified as relevant so far as developments of AI oriented technologies are concerned.

They are (i) Health, (ii) Manufacturing (iii) Fin-Tech (iv) Agriculture, (v) Education, (vi) Environment, (vii) Public Utility Services, (viii) Technology for disabled persons (ix) National Security and (x) Customer Relationship Management (CRM).

b) The report of the task force has identified some specific challenges contemplated to be faced while deploying AI algorithms on a large scale in India in different above-mentioned sectors. They are mainly (i) How huge data collection and its analysis through AI can be safeguarded so that privacy is not at stake (ii) How data security, privacy, ethical norms can

[5] Writ Petition (Supreme Court) (Civil) No.494 of 2012.
[6] http://dipp.nic.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf (Last accessed on December 27, 2018.)

 [ISSN 2581-5369]

be ensured with the help of technological framework and regulatory framework (iii) How excessive but effective use of AI in different fields would affect the issue of employment curtailment and (iv) How and to what extent digitalization through the help of use of AI in the form of application of Internet of Things (IoT) would be vulnerable in the light of cyber attacks.

(B) Recommendations

1. The task force has recommended to set-up an 'Inter Ministerial National Artificial Intelligence Mission' to act for a period of 5 years. It is to be funded for about 1200 Crores (INR). This will be acting as a Nodal Agency (NA) to monitor and co-ordinate all the technological activities involving use of AI in India.

This Mission will involve its activities in three major sectors.

i) To bring all the academicians and industry players to arrange to store all the AI related research works and to appropriately fund to enhance studies on AI in national level and to develop awareness on utility of AI in the society.

ii) To establish co-ordination among different Ministries for expanding use of AI systems in India.

iii) To set up Centres of Excellence for boosting up research facilities and to establish generic testing procedure to assess AI performance and to fund for developing an autonomous AI machine for providing appropriate information to the public to enrich them.

2. The taskforce has recommended to ensure preservation policy of data and to ensure proper prescription for standardization of data. The task force has prescribed:

(i) To set up digital data banks for getting cross-industry data. (ii) To create a data-ombudsman by the Ministry of Commerce and Industry for addressing data related issues while dealing with data by AI. (iii) Bureau of Indian Standards (BIS) should take initiative for implementing norms and standards which are internationally discussed in the light of AI systems.

3. Two specific policies are to be framed. They are: (i) Policy dealing with data. (ii) Tax-incentives concerning to income produced from the use of AI technologies.

4. To strategize for developing enough human resources to meet growing demand for dealing with AI algorithms.

5. Inter departmental co-ordination is to be established so that India can take part in International Discussion Forum on AI applications.

 [ISSN 2581-5369]

From the studies of recommendations by the task force, it appears that the recommendations are well-knit and well-thought. It would appropriately encourage the growth of use of AI oriented technologies. At the same time, it will be able to manage data protection issues. Again, in the light of verdict of the Apex Court of India regarding declaration of right to privacy as a constitutional fundamental right,[7] a data protection framework is needed to be formulated as observed in the judgement. In conformity with this verdict of the Apex Court of the country, Ministry of Electronics and Information Technology (MeitY) has formed a committee headed by Hon'ble B.N. Srikrishna J for identifying key issues concerning to data protection and to recommend executable mechanisms.

This is for addressing those issues and to provide a draft for data protection bill scheduled to be introduced in the Parliament of India to make the bill into an enactment.

We are hoping that the outcome of the recommendations of task force and this data protection bill will simultaneously be able to plug up the lacunas and applications of AI will not jeopardise the privacy protection of personal data when there will be frequent applications of AI in India.

V. Artificial Intelligence and Data Protection in India.

It is observed that technology under different ramifications is permeating in the Indian society in a rapid pace. It is noted that many usable devices are becoming smarter as they are being connected with Internet leading to the way to establish Internet of Things (IoT) region (Kumar et al., 2017; Lord, 2013; McWhorter, 2017). Within a very short time, it is expected that AI would cover all our smart technological activities.

This increasing involvement of applications of AI algorithms in functions like data analysis, employment field, healthcare sector, IoT areas, transportation sector and so on will lead the AI to be able to have easy access to Personally Identifiable Information (PII). This would help business organizations to have an idea regarding the preferences of the potential consumers. It highlights the extent of impact of AI on PII. Data analysis is being done by AI for different purposes beneficial for the society. However, such easy access to personal data by AI also invites larger questions concerning to privacy issues. Hence, a comprehensive framework and effective policy are to be framed to address the privacy vulnerabilities to control the use and applications of AI. This concern has become more important in view of the recent judgement of the Supreme Court of India wherein it has been held inter alia that privacy is a fundamental constitutional right. The Apex Court in that revolutionary order has

[7] Writ Petition (Civil) NO.494 of 2012 (Supreme Court of India).

 [ISSN 2581-5369]

also observed that there is a need to provide a technology-neutral framework that would be able to encompass important privacy-concern issues instrumental to the use of AI in India (Gomory, 2000; Kumar et al., 2018).

We have already given a concise primer on the framework concerning the data protection. Still, the Apex Court of India in the afforested judgement has emphasized the need of providing a more exhaustive and comprehensive data protection framework presumably thinking that the existing legal mechanisms to combat data protection privacy are not adequate. In terms of provisions of Information Technology Act, 2000, a rule in the name. Sensitive Personal Data or Information (SPDI) Rules, 2011 has been framed. However, this rule deals with the issue of compensation when reasonable security practices are not maintained to protect sensitive information. But, these information do not include the information provided to the applicants in terms of Right to Information Act, 2005.[8] However, recently several questions have cropped up regarding the effectiveness of this rule since it includes protection to a certain kind of information. It does not protect that information which are not covered by this rule. Hence, it is construed to be not generic to protect all types of data (Brynijolffson and McAfee, 2014; Herzog, 2016).

Thus, existing data protection enactment and rules as mentioned above are felt not adequate to combat effective protection to privacy of personal data and presumably that is why the Apex Court in the afforested Judgement has mentioned the need of framing more exhaustive and comprehensive data protection legal mechanisms.

Following the observation of Apex Court, the Government of India through different departments have set up the task force and a committee under the Chairmanship of Prof. V. Kemakoti and Hon'ble Justice B. N. Srikrishna respectively details of which have already been mentioned. All these efforts are being made to provide executable, comprehensive legal framework for ensuring effective protection of privacy of personal data, especially when they are being dealt with by AI mechanisms.

VI. APPLICATION OF AI AND ITS LIABILITY

The AI is being used universally in this modern technological ambience. In this perspective, it is very relevant to think to fix liability on the application of AI if it causes harm or damage. However, this assignment of liability is considered as an important issue in granting a legal personality to AI. The normal conception is that the AI cannot be held responsible and liable

[8] Provisions of rule 3 of I.T. (Reasonable Security practices and procedures and Sensitive Personal Data or Information) Rules, 2011.

for causing any damage in its own capacity because AI can hardly qualify itself to possess legal personhood. It is natural that robots can never be sued though they can do harm and damage. However, introduction of AI has prompted the stakeholders to rethink this normal conception that machines cannot have legal personality (Solum, 1992). In this light, sense of liability covers a question in the perspective of extent of legal relationship between AI and its actual developer. Jurisprudence says that unlawful actions causing damages are needed to be compensated. These liabilities are of two types: Civil Liabilities & Criminal Liabilities (Wakabayashi, 2018).

(A) Civil Liabilities

Damage is considered as one of the principal ingredients of civil liability[9] as suggested by Paulius Cerka et al.[10] Damage caused is to be proved first for getting redressal. For argument sake, we can say if AI possesses super-intelligence, then AI is supposed to be aware of its actions. Again, if it is considered that AI is aware of its action, it is natural to infer that AI is also liable for its actions. Hence, AI is supposed to have possessed rights and duties which are generally attributed to both types of legal persons – humans as well as artificial like corporation. This invites a question if AI can be attributed with personhood.[11]

At this moment, it has no answer but with passage of time it is certain that jurisprudence would be able to evolve an acceptable logical answer. In case of accidents occurring in self driving cars driven with the help of AI, discussions are on the legal table if AI or its developers be fixed with civil liabilities to cause damage.

(B) Criminal Liabilities

Applications of AI have become an integral part of our daily life.[12] But, ironically, it has become a burning question if AI would pose a threat to human lives. Over more than 1000 research papers including research papers of Stephen Hawking during 2015 highlighted that destruction might have been caused through AI warfare.[13] In case AI causes such harm, question arises that how the situations can be controlled through laws or through ethics. It has been observed that problem is that AI entities are not considered as a subject to the law. This

[9] "Artificial Intelligence, Legal Responsibility and Civil Rights" by Christoffer O. Hernees. This is available at https://techcrunch.com/2015/08/22/artificial-intelligence-legal-responsibilityand-civil-rights/
[10] "Liability for Damages caused by Artificial Intelligence" written by Paulis Cerka et al. It is available at http://fulltext.study/download/467680.pdf. (Last accessed on November 10, 2018.)
[11] "Legal Personhood for Artificial Intelligences". Written by L. B. Solum (1992). North Carolina Law Review.
[12] "Thinking Supercomputer Now Conscious as a Cat" written by Chris Capps. It is available at http://www.unexplainable.net/artman/publish/article_14423.shtml
[13] "Hawking, Musk Warm of Virtually Inevitable Al Arms Race" composed by Lucas Matney. It is available at https://techcrunch.com/2015/07/27/ artificially-assured-destruction/#.woknrl:EnLr. (Last accessed on December 22, 2018.)

question was raised by Gabriel Hallevy.[14] However this dilemma has been contrasted in the same manner as was done when question of commission of crime was considered committed by corporation (artificial subject).[15] It is a fact that basically an entity may be brought under ambit of criminal laws if two basic requirements are fulfilled. These are actus reus (criminal conduct) and mens rea (mental or internal element). However, Hallevy has considered three criteria to bring AI under criminal liabilities. These are: (i) AI is not ascribed with human attributes. AI is not considered to possess criminal state of mind. It has been noted that the real perpetrator is that person who is responsible for commission of the offence. Perpetrator is either the end user or the programmer responsible to device the AI software. (ii) The end user or the programmer of the AI algorithm is to shoulder criminal liability without having criminal intention. This liability is fixed on them considering their negligent mental state. (iii) In this concept, AI is directly charged to shoulder criminal liability. In this model AI is held criminally liable along with the end users or the programmers.

However, when case of criminal liability of AI is considered, these three cases are to be accounted simultaneously. Liability is to be assessed in the light of the specific context.

VII. CONCLUSION

In various economies throughout the globe, use of AI is being increased with rapid pace. Consequently, individuals and entities are more and more depending on AI. This dependency on AI by individuals or by entities is expected to increase rapidly with passage of time. This idea is evidenced from the fact that application of AI would bring in economic growth to the tune of 1.7% (average growth) throughout different industries by 2035.[16] However, integration and development of use of AI algorithms with industrial sectors and social sectors instrumental for improving the economic health of India will be interrupted if the concerns regarding protection of personal data privacy is not properly looked into and is not appropriately addressed. In this context, the most important thing is the issue of fixation of civil or criminal liabilities on AI in case such application of AI causes damages or causes an offence detrimental to the interest of the society. This will ensure the issue of soothing as well as close relationship ensuring resonance among law, ethics and AI.

In order to combat the situation, the regulatory authorities of India are supposed to adopt a

[14] "The Criminal Liability of Artificial Intelligence Entities-From Science Fiction to Legal Social Control". It is written by Gabriel Hallevy.
[15] "No Soul to Damm: No Body to Kick: An Uncanndalised Inquiry into the Problem of Corporate Punishment." It is written by John C. Coffee, Jr. 79 MICH.L.REV.386 (1981).
[16]https://www.forbes.com/sites/louiscolumbus/2017/06/22/artificial-intelligence-will-enable-38-profit-gains-by-2035/#2f7f-30da1969, (Last accessed on November 19, 2018.)

 [ISSN 2581-5369]

balanced and calibrated approach between the necessary protection of privacy of personal data of citizens as well as to effectively encourage the growth of technology especially the use of AI technology. If it is not ensured, that is, if such balance is not established between these two issues, it might either adversely affect the privacy vulnerabilities of individuals so far as their personal data are concerned or it may adversely retard the technological growth of India culminating retardation on the overall growth of this country.

This would have also negative impact on revelation of innovative activities which is undesirable. The regulations should be such as these would effectively guide the end users or programmers of AI algorithms so that they are strictly bound to adhere to the ethical standards while programming AI algorithms (Wiegel, 2010). In India, still due to lack of effective jurisprudence to ensure balance between privacy issues and essential usage of AI technology, it is expected that in a near future appropriate, comprehensive, executable, simple enactments, rules and policies would be formed so that through increased use of AI applications, the technological growth would reach apex of its success without compromising with the protection of data privacy issues.

*****

 [ISSN 2581-5369]

VIII. REFERENCES

1. Autor DH, Levy F and Murnane RJ (2003) The skill content of recent technological change: an empirical exploration. The Quarterly Journal of Economics 118(4): 1279-1333
2. Barrat J (2013) Our final invention: artificial intelligence and the end of the human era. Thomas Dunne Books, New York
3. Bhattacharya, K. & Chatterjee, S. (2020). Adoption of artificial intelligence in higher education: a quantitative analysis using structural equation modelling", *Education and Information Technologies*, In Press. https://doi.org/10.1007/s10639-020-10159-7.
4. Bostrom N (2016) Superintelligence: paths, dangers, strategies. Oxford University Press, Oxford
5. Brown N and Sandholm T (2018) Superhuman AI for heads-up no-limit poker: libratus beats top professionals. Science 359(6374): 418-424.
6. Brynjolffson E and McAfee A (2014) The Second Machine Age: Work, Progress, and Prosperity in a time of Brilliant Technologies. W.W. Norton & Company, New York, NY.
7. Chace C (2015) Surviving AI. Three Cs, Bradford
8. Chatterjee, S (2019), "Artificial Intelligence and Human Rights: From Socio-Legal Perspectives", *International Conference on Law and Technology [ICLT 2019]*. School of Law, The University of Petroleum & Energy Studies (UPES), Dehradun, Uttarakhand, India. 28-29 September 2019.
9. Chatterjee, S. (2011), "Organization learning and learning organization: A critical review - A Paradox", *Asian Journal of Computer Science and Information Technology*. Vol. 1 No. 3, pp. 64-70. ISSN: 2249-5126.
10. Chatterjee, S. (2015). "Security and privacy issues in E-Commerce: A proposed guidelines to mitigate the risk", *IEEE International Advance Computing Conference (IACC).* pp. 393-396. https://doi.org/10.1109/IADCC.2015.7154737.
11. Chatterjee, S. (2016). "A synthesis of structural creative problem solving in the perspective of OR/MS methodology", *International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT).* pp. 1-6. https://doi.org/10.1109/ICCTICT.2016. 7514614.
12. Chatterjee, S. (2018), "Data Privacy and Intellectual Property Rights in Cyberspace", *Legal Research Development: An International Refereed e-Journal*. Vol. 2 No. 3, pp. 42-49. ISSN: 2456-3870.

13. Chatterjee, S. (2018), "Internet of Things and Social Platforms: An empirical analysis from Indian consumer behavioral perspective", *Journal of Behavior & Information Technology*, Vol. 39 No. 2, pp. 133-149.
14. Chatterjee, S. (2018). "Law and Social Cohesion: A chronological overview from India perspective". *International Journal of Research in Social Sciences*. Vol. 8 No. 3, pp. 204-216. ISSN: 2249-2496.
15. Chatterjee, S. (2018). "Privacy, Human Behavior and Fundamental Rights in India: Some recent development and analysis", *Indian Journal of Law and Human Behavior*, Vol. 4 No.1, pp. 95-103. ISSN: 2454-7107.
16. Chatterjee, S. (2019), "Antecedence of attitude towards IoT usage: A proposed unified model for IT Professionals and its validation", *International Journal of Human Capital and Information Technology Professionals*, Vol. 18 No. 1, Article 4.
17. Chatterjee, S. (2019), "Antecedents of behavioral intention impacting human behavior to use IoT enabled devices: An empirical investigation", *International Journal of Technology and Human Interaction*. Vol. 18 No. 1, Article 4.
18. Chatterjee, S. (2019), "Emergence of AI and its implication towards data privacy: From Indian legal perspective", *International Conference on Justice Education: Artificial Intelligence and Its Legal Implication [ICJE 2019]*. Institute of Law, Nirma University, Ahmedabad, Gujrat, India. 15-16 March 2019.
19. Chatterjee, S. (2019), "Factors Impacting Behavioral Intention of users to adopt IoT in India: From Security and Privacy Perspective", *International Journal of Information Security and Privacy*. Vol. 14 No. 4, Article 6.
20. Chatterjee, S. (2019), "Impact of AI regulation on intention to use robots: From citizens and government perspective", *International Journal of Intelligent Unmanned Systems*, Vol. 8 No. 2, pp. 97-114. https://doi.org/10.1108/IJIUS-09-2019-0051.
21. Chatterjee, S. (2019), "Why people will use IoT enabled devices? An empirical examination from Indian perspectives", International Journal of Technology and Human Interaction, Vol. 18 No.2. Article No. 7.
22. Chatterjee, S. (2019). "AI strategy of India: policy framework, adoption challenges and actions for government", *Transforming Government: People, Process and Policy*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/TG-05-2019-0031.
23. Chatterjee, S. (2019). "Determinants impacting diffusion of knowledge in higher learning institutes in India: an empirical study", *Journal of Studies in Higher Education*, Earlysite. https://doi.org/10.1080/03075079.2019.1599847.

24. Chatterjee, S. (2019). "Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective", International Journal of Law and Management, Vol. 61 No. 1, pp. 170-190. https://doi.org/10.1108/IJLMA-01-2018-0013.
25. Chatterjee, S. (2020), "Antecedents of phubbing: from technological and psychological perspectives", *Journal of Systems and Information Technology*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JSIT-05-2019-0089.
26. Chatterjee, S. (2020). *Critical Success Factors to Create 5G Networks in the Smart Cities of India From the Security and Privacy Perspectives*. Chapter 10. In the book of Novel Theories and Applications of Global Information Resource Management by Zuopeng Zhang. IGI Global, USA Publication. https://doi.org/10.4018/978-1-7998-1786-4.ch010. ISBN13: 9781799817864.
27. Chaudhuri, R. & Chatterjee, S. (2010), "A system theoretic analysis of IT/IS outsourcing: A case-based approach", *Journal of Modeling and Simulation of Systems*. Vol. 1 No. 2, pp. 131-143.
28. Chaudhuri, R. & Chatterjee, S. (2013), "Information-Knowledge Space: A Transformation Model for IT and other knowledge Intensive organizations", *Global Journal of Management and Business Research*, Vol. 13 No. 1, pp. 42-52.
29. Chaudhuri, R. & Chatterjee, S. (2013), "System and Process Analysis of IT/IS Outsourcing in Japanese Market: Opportunities for India", *Global Journal of e-Business & Knowledge Management*. Vo. 5 No. 1, pp. 8-19.
30. Chaudhuri, R., Chatterjee, S., & Ghosh, S.K. (2019), "Adoption of Ubiquitous Customer Relationship Management (uCRM) in Enterprise: Leadership Support and Technological Competence as Moderators", *Journal of Relationship Marketing*. Vol. 19 No. 2, pp. 75-92. https://doi.org/10.1080/15332667.2019.1664870.
31. Chen N (2018) Are robots replacing routine jobs? Harvard College Thesis, Applied Mathematics Cambridge, MA, March 30.
32. Chopra S and White L (2004) Artificial agents—personhood in law and philosophy. In: De Mántaras RL, Saitta L (eds) The 16th European conference on artificial intelligence, Valencia, 22–27 Aug 2004
33. Chopra S and White L (2011) A legal theory for autonomous artificial agents. The University of Michigan Press, Ann Arbor
34. Garner R (2005) The political theory of animal rights. Manchester University Press, Manchester

35. Ghosh, S.K., Chatterjee, S., & Chaudhuri, R. (2019), "Knowledge Management improving Business Process: An interpretative framework for successful implementation of AI-CRM-KM System in organizations", *Business Process Management Journal*, https://doi.org/10.1007/s40171-017-0173-5.
36. Ghosh, S.K., Chaudhuri, R. and Chatterjee, S. (2019), "Adoption of AI-Integrated CRM System by Indian Industry: From Security and Privacy Perspective. Information and Computer Security.
37. Ghosh, S.K., Chaudhuri, S., Vrontis, D., & Thrassou, A. (2020), "Social customer relationship management factors and business benefits", *International Journal of Organizational Analysis*, In press.. https://doi.org/10.1108/IJOA-11-2019-1933.
38. Gomory RE and Baumol WJ (2000) Global Trade and Conflicting National Interests. MIT Press, Cambridge, MA.
39. Gupta, M.P., Chatterjee, S. & Kar, A. (2018), "Success of IoT in Smart Cities of India: An empirical analysis", *Government Information Quarterly*. 35(3), 349-361. https://doi.org/10.1016/j.giq.2018.05.002.
40. Gupta, M.P., Chatterjee, S. & Kar, A.K (2017). Critical Success Factors to Establish 5G Network in Smart Cities: Inputs for Security and Privacy. *Journal of Global Information Management*, 25(2), 5-37. https://doi.org/10.4018/JGIM.2017040102.
41. Gupta, M.P., Chatterjee, S. & Kar, A.K. (2018). Alignment of IT authority and citizens of proposed smart cities in India: System security and privacy perspective", *Global Journal of Flexible Systems Management*. 19(1), 95-107. https://doi.org/10.1007/s40171-017-0173-5.
42. Hallevy G (2010) The criminal liability of artificial intelligence entities—from science fiction to legal social control. Akron Intellect Prop J 4:171–201
43. Herzog W (2016) Lo and behold, reveries of the connected world [film]. Saville Productions, Los Angeles
44. Kar, A.K. (2019) & Chatterjee, S. Securing IoT devices in Smart Cities of India: From ethical and enterprise information system management perspective. *Journal of Enterprise Information System*. In Press. https://doi.org/10.1080/17517575.2019.1654617.
45. Kassaro TM and Norton H (2016) Siri-ously? Free speech rights and artificial intelligence. Northwest Univ Law Rev 110:1169–1194

46. Kraakman R, Armour J, Davies P, and Enriques L (2017) The anatomy of corporate law: a comparative and functional approach. 3rd edn. Oxford University Press, Oxford
47. Kritzer N (2015) Cat picture please. Clarkesworld 100
48. Kumar, A.K. & Chatterjee S. (2017). *Smart Cities in India: A Conceptual framework for emerging economics focusing on security and privacy aspects*, Advances in Theory and Practice of Emerging Markets Book Series. Springer Publication. Status: Submitted, awaiting review.
49. Kumar, A.K. & Chatterjee, S. (2018). Effects of successful adoption of information technology enabled services in proposed smart cities of India: From user experience perspective. *Journal of Science and Technology Policy Management*, 9(2), 189-209. https://doi.org/ 10.1108/JSTPM-03-2017-0008.
50. Kumar, A.K. & Chatterjee, S. (2018). Regulation and governance of the Internet of Things in India. *Journal of Digital Policy, Regulation and Governance.* 20(5), 399-412. https://doi.org/10.1108/DPRG-04-2018-0017.
51. Kumar, A.K., & Chatterjee, S. (2016). *Concept of Smart Village in India: A literature Review and Policy Insights*, International Conference on Smart Cities, ICEG, IIT Delhi, India.
52. Kurki VAJ and Pietrzykowski T (eds) (2017) Legal personhood: animals, artificial intelligence and the unborn. Springer, Cham
53. Lawless WF and Sofge DA (2017) Evaluations: autonomy and artificial intelligence: a threat or savior? In: Lawless WF, Mittu R, Sofge D, Russell S (eds) Autonomy and artificial intelligence: a threat or savior? Springer, Cham
54. Lee P and George RP (2008) The nature and basis of human dignity. Ratio Juris 21:173–193
55. Leenes R and Lucivero F (2014) Laws on robots, laws by robots, laws in robots: regulating robot behavior by design. Law Innov Technol 6:193–220
56. Lord N (2013) Regulating transnational corporate bribery: anti-bribery and corruption in the UK and Germany. Crime Law Soc Change 60:127–145
57. McWhorter JH (2017) Words on the move: why English won't—and can't—sit still (like, literally). Picador, Henry Holt and Company, New York
58. Misra, S., Majumdar, D., Chatterjee, S. & Damaševičius, R. (2019), "Adoption of mobile applications for teaching-learning process in rural girls' schools in India: an

empirical study", *Education and Information Technologies*, In Press. https://doi.org/10.1007/s10639-020-10168-6.

59. Moravčík M, Schmid M, Burch N, Lisý V, Morrill D, Bard N, Davis T, Waugh K, Johanson M and Bowling M (2017) DeepStack: expert-level artificial intelligence in heads-up no-limit poker. Science 356 (6337): 508-513
60. Nguyen, B. Chatterjee, S., Ghosh, S., & Chaudhuri, R. (2019). "Are CRM systems ready for AI integration?", *The Bottom Line*, Vol. 32 No. 2, pp. 144-157. https://doi.org/10.1108/BL-02-2019-0069**.**
61. Roberts R (2014) How Adam Smith can change your life: an unexpected guide to human nature and happiness. Penguin, New York
62. Sheshadri, C. (2015), "ERP System and Business Transformation: An investigative Analysis of Success and Failure for Organizations", *International Journal of Science Technology & Management.* Vol. 4 No. 2, pp. 197-206.
63. Sheshadri, C. (2015). "E-Commerce in India: A review on culture and challenges", *IEEE International Conference on Soft Computing Techniques and Implementations (ICSCTI).* pp. 105-109. https://doi.org/10.1109/ICSCTI.2015.7489547.
64. Sheshadri, C. (2015). "ERP failure in developing countries: A case study in India", *2015 Annual IEEE India Conference (INDICON).* pp. 1-6. https://doi.org/10.1109/INDICON.2015. 7443222.
65. Sheshadri, C. (2017), "Issues of personal data protection and privacy in cyberspace: A comparative analysis among different countries", *International Journal of Law*, Vol. 4 No. 2, pp. 01-08. ISSN: 2455-2194.
66. Sheshadri, C. (2017), "Surveillance Threating Privacy and Data Protection: A Review", *International Journal of Current Trends in Science and Technology*, Vol. 8 No.3, pp. 20583- 20590. ISSN: 0976-9498. https://doi.org/10.15520/ctst.v8i03.360.
67. Sheshadri, C. (2019), "Critical issues with Artificial Intelligence, Blockchain and Personal Data: From Social, legal and Policy perspective", *Blockchain Technology: Adoption, Regulation & Security*. National Law Institute University, Bhopal, India. 18-19 October 2019.
68. Sheshadri, C. (2019), "Influence of IoT policy on Quality of Life: From Government and Citizens' perspective", *International Journal of Electronic Government Research*, Vol. 15 No. 2, pp. 19-38; https://doi.org/10.4018/IJEGR.2019040102.
69. Sheshadri, C. (2019), "Issues of Human Rights in the era of Artificial Intelligence: From Regulation and Policy Perspective", *Advancements in Legal Research:*

Reflections in Contemporary Pandemic and Transdisciplinary Dimensions, Amity Law School, Amity University, Noida, Uttar Pradesh, India. 4-5 October 2019. ISBN: 978-16-92702-10-6.

70. Sheshadri, S. (2019), "Artificial Intelligence and Personal Data: From Legal and Policy Perspective", *International Conference on Digital Transformation: A Cognitive learning towards artificial intelligence [ICDT 2019]*. Rajiv Gandhi National University of Law, Patiala, Punjab, India. 6-8 September 2019. pp. 409-417. ISBN: 978-93-83043-28-6**.**

71. Solaiman SM (2016) Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy. Artif Intell Law 25:155–179

72. Solum LB (1992) Legal Personhood for Artificial Intelligences. North Carolina Law Review 70:1231-1287.

73. Teubner G (2006) Rights of non-humans? Electronic agents and animals as new actors in politics and law. J Law Soc 33:497–521

74. Vladeck DC (2014) Machines without principals: liability rules and artificial intelligence. Wash Law Rev 89:117–150

75. Wakabayashi D (2018) Self-driving Uber car kills pedestrian in Arizona, where robots roam. https :// www.nytim es.com/2018/03/19/techn ology /uber-drive rless -fatal ity.htm. Accessed 18 June 2018

76. Wiegel V (2010) The ethics of IT-artefacts. In: Floridi L (ed) The Cambridge handbook of information and computer ethics. Cambridge University Press, Cambridge 201–218.

*****