ARTIFICIAL INTELLIGENCE IN HEALTH CARE SECTOR OF INDIA: LEGAL REGULATORY CHALLENGES & WAY FORWARD

Written by ***Sheikh Sultan Aadil Huque* & Mahwesh Buland*****

**LLM-PhD Scholar, National Academy of Legal Studies & Research (NALSAR), Hyderabad*

***5th Year BBA LLB, KIIT School of Law, KIIT University, Bhubaneswar*

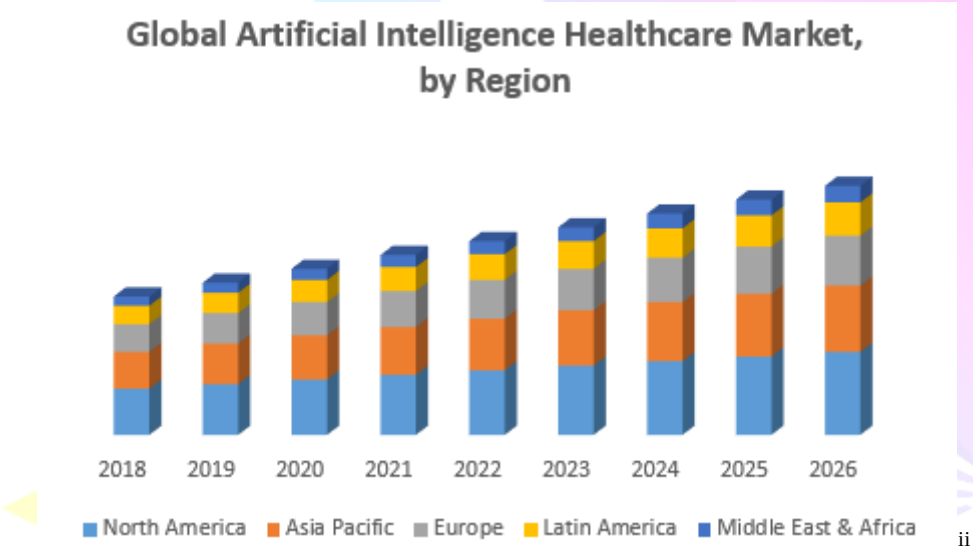
ABSTRACT

Though there is potential for AI to transform healthcare in India, ethical, legal, and cultural factors need to be considered by developers, practitioners, and policy makers when designing, using, and regulating AI. But there are some major regulatory issues of concern with respect to AI in health care like: How do AI programs ensure patient consent and privacy of sensitive medical data? How to address the questions of apportionment of liability among the practitioner, hospital, and the AI system developer, trainer and manager in case of an act of medical negligence? Further in the event of an AI diagnostic error how to determine the degree of accountability of the operating physician when a wrong diagnosis or treatment occurs due to an error in the primary data feed or an AI systemic glitch? With all this issues in hand & with the advancement of AI in health care, this paper aims to seek a review of India's existing legal framework & AI policy regulation and how far are they efficient enough in addressing the intrinsic issue which might make the journey of AI in regulatory terms bit cumbersome. The paper will also analyse the steps taken by European Union in regulation of AI in health care and how India can learn from world best practices in order to come up with a robust & fair regulatory mechanism.

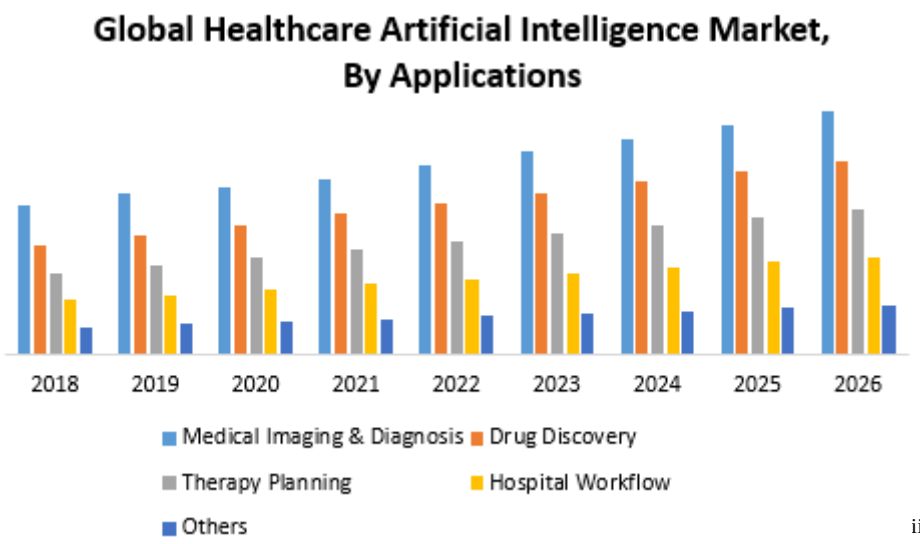
***Keywords*:** Artificial Intelligence (AI), Health Care, Intermediary Liability, Privacy, Health Data, Medical Negligence, Policy Regulations, Accountability.

ARTIFICIAL INTELLIGENCE IN HEALTH CARE SECTOR

With India's untenable patient-doctor ratio, global analysts expect that the pressure to improve healthcare delivery will lead to a faster inclusion of Artificial Intelligence (AI) and Deep Learning (DL) into the country's existing diagnostic and treatment processes. Artificial Intelligence has the potential to provide large incremental value to a wide range of sectors globally, and is expected to be the key source of competitive advantage for firms. While advancements in AI are India's best bet yet to sustain its crumbling healthcare infrastructure, visionless implementation of AI medical technology and the absence of a robust legal framework can only compound the crisis, and not mitigate it. These kinds of technologies may increase patient safety and help to control, for example, the use of antibiotics to reduce antimicrobial resistance.[i]



[ii]



[iii]

As, we can see from the above data, how rapidly the AI in health care sector is growing rapidly and is being used in various forms. Yet, they also raise concerns and challenges with regard to safety, effectiveness, transparency, data sharing, property rights, antitrust, cyber security, privacy, and algorithmic bias and discrimination.[iv] Hence, though there is potential for Artificial Intelligence to transform healthcare in India, ethical, legal, and cultural factors need to be considered by developers, practitioners, and policy makers when designing, using, and regulating AI. Electronic storage of medical records has exposed individuals to the risk of identification at various stages of data collection and data processing.[v] Following are some of the major regulatory issues of concern with respect to AI in health care:

1. *How do Artificial intelligence programs ensure patient consent and privacy of sensitive medical data?*

2. *How to address the questions of apportionment of liability among the practitioner, hospital, and the artificial intelligence system developer, trainer and manager in case of an act of medical negligence?*

Hence, there is an urgent need for the policy makers, healthcare AI developers, and medical practitioners in India to consider the legal aspects while designing, implementing, and regulating artificial intelligence in the healthcare sector.

COMPARATIVE INSTITUTIONAL ANALYSIS

While the application and challenges from AI development are global in nature, however the regulatory approaches taken by countries vary. For, example, European Union took the lead in formulating and enacting a detailed regulation on data usage and privacy in the world. In contrast US are seen as a country that follows the principle of light touch regulation.[vi] Some countries are in the process of designing guidance documents as general principles of governance. The other alternative to this is to adopt a more ex post reactionary approach and develop regulation on the go as responses to practical interactions. The trade-off is between addressing the potential harms vs. possibly stifling development of these technologies.[vii]

Coming to Indian context, it lacks a regulating authority for AI in healthcare. Broadly speaking, the Information Technology Act, 2000 is the only piece of legislation which 'touches' upon this subject. Whereas it is undeniable that certain safeguards pertaining to data protection and privacy have been laid down in Sections 43A and 72 of the Act, but the safeguards fall greatly short of ensuring actual protection because of the obscure nature of provisions, added majorly through amendments.[viii] So, when we talk of health care, The Central Drug Standards Control Organisation (CDSCO) is the prime regulatory authority which looks into provisions of The Drugs and Cosmetics Act, 1940 and Rules thereof. Further, the practice of medicine is regulated by the Medical Council of India. So, the possible options include the Medical Council of India (National Medical Commission), the Drug Controller General of India, or a new entity established specifically for this area.[ix] A possible alternative could be empowering the MCI to oversee the medical aspects, and a regulator under the Data Protection Bill to oversee issues relating to data. There is also a regulatory gap around medical devices, which has sought to be addressed by the recent Indian Medical Devices Rules, 2017.

EXISTING STANDARDS

Information Technology Act, 2000; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:

The use of these new technologies requires a constant exchange of information between the patient and the service provider. The patient's personal information, such as medical history and physiological conditions, are considered Sensitive Personal Data or Information ("SPDI") under the Data Protection Rules ("Rules"), of which certain provisions apply when a body corporate collects, stores, transfers or processes such information. Consent is a clear requirement under the Rules.[x] However, despite the existence of these rules, there has been minimal compliance in India due to lack of enforcement mechanisms. Questions have also been raised about the legislative scope of these rules which while drafted under a data security provision, may be seen as going beyond its scope. Section 79 of the Act suggests that intermediary service providers in the field of information technology are merely the carriers of content. Barring exceptions, under Section 79, they would not be held liable for the substance of the content.[xi] This rule may have to be re-examined with the implementation of AI systems that are devised by the carriers. Further, data localisation will be of prime concern in case of devices manufactured outside India.

Electronic Health Records Standards, 2016:

The EHR Standards are an attempt to regulate data ownership and privacy standards around the storage of health data collected from patients. This includes data from medical establishments as well as data from medical devices and self-care devices and systems. The government has recognised the need for standardisation of such data, and has accordingly laid down standards relating to information capture, storage, retrieval, exchange and analytics, including images, clinical codes and data. These include ISO and other national standards to be used for EHRs.[xii] In the latest review report prepared by the ministry of electronics and information technology (MeitY) titled Adoption of Electronic Health Records: A Roadmap for India highlighted that the government hospitals and dispensaries have very little ICT infrastructure with only some major public hospitals, such as the All India Institute of Medical Sciences (AIIMS) and the Postgraduate Institute of Medical Education and Research (PGIMER), have computers and connectivity.[xiii] Except for a handful of large healthcare organizations in India, there has not been a major effort towards EHR implementation. Thus, when we lack in terms of basic infrastructure the adoption and implementation of the same is highly doubtful and risky.

Medical Devices Rules, 2017

It has been drafted with the intention to distinguish between medical devices and pharmaceuticals for the purpose of regulation. The Rules define what shall be classified as medical devices, and the scope of these Rules is limited to those devices that fall within its ambit. The Rules do not contain separate provisions for sale of medical devices.[xiv] The slow pace and method of medical device regulation has been a concern for the industry for a while now, and the Draft Notification is a means of extending the regulatory ambit of the MDR.[xv]

Digital Information Security in Healthcare Act (DISHA):

The MoHFW created the draft for the Digital Information Security in Healthcare Act (DISHA) with the aim of securing the healthcare sector data in India, giving people complete ownership of their health data. For example, if you are visiting a doctor for a check-up and the doctor places your results into an electronic health record (EHR) that information is completely protected by DISHA as it is placed within the healthcare system.[xvi] DISHA proposes three main objectives such as: setting up a digital health authority at national and state levels; enforcing privacy and security measures for electronic health data; and regulating the storage and exchange of electronic health records. Additionally, the draft also provides details on the establishment of National and State Electronic Health Authorities (NeHA and SeHA). In effect, it would provide extensive data protection to Indian subjects, as well as govern the data portability. But it still has certain inherit flaws like the patient seems to be the focal point of DISHA. Throughout the act, there is much power given to the patient over his/her medical data and very rightfully so. However, it is unclear of how will a nation having over a billion people be educated about a) rights over the data b) need for consent c) how and when to decide to provide or reject consent d) what is the mode for receiving and auctioning on a consent request and many more such important aspects.[xvii]

STEPS TAKEN BY EUROPEAN UNION TO REGULATE AI IN HEALTH CARE

In February, 2020, the European Commission published a white paper on artificial intelligence (AI) as well as an accompanying communication and report. It aims to pursue a uniform approach to AI across the EU in order to avoid divergent member state requirements forming barriers to its single market. The paper sets out policy options to facilitate a secure and trustworthy development of AI and considers health to be one of its most important areas of application.[xviii] The white paper distinguishes high-risk AI applications from all other AI applications, with the aim of applying the new regime of regulation and conformity assessment only to the high-risk applications. According to the paper, high-risk AI applications are those used in a sector where "significant risks can be expected." The legislation establishing the new regulatory framework should "specifically and exhaustively" list the high-risk sectors, which might initially include "healthcare".[xix] Some of the relevant portions from the white paper with respect to regulation of AI in health care are as follows:

Certification:

The commission also plans to offer a "trustworthy AI" certification, to encourage voluntary compliance in low-risk uses. Certified systems later found to have breached the rules could face fines. Further, it provides for the training data requirements would aim at "providing reasonable assurances that the subsequent use of the products or services that the AI system enables" would be safe, non-discriminatory and protective of privacy. Developers or deployers of AI systems would need to demonstrate, for instance, that their proposed AI systems "are trained on data sets that are sufficiently broad and cover all relevant scenarios needed to avoid dangerous situations." In addition, the data sets must be "sufficiently representative, especially to ensure that all relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination are appropriately reflected."[xx]

Issue of Privacy Concerns:

The white paper recommends no new specific requirements to ensure that proposed AI systems adequately protect personal data, instead suggesting that these issues can be addressed under the GDPR and its companion law enforcement data privacy directive. Record-keeping rules

would be imposed "in relation to the programming of the algorithm, the data used to train high-risk AI systems, and, in certain cases, the keeping of the data themselves." [xxi]

Developers and deployers of high-risk AI systems must provide information concerning the "AI system's capabilities and limitations, in particular the purpose for which the systems are intended, the conditions under which they can be expected to function as intended and the expected level of accuracy in achieving the specified purpose." In addition, "citizens should be clearly informed when they are interacting with an AI system and not a human being. "The paper states that, the commission will draft new laws including a ban on "black box".AI systems that humans can't interpret to govern high-risk uses of the technology, such as in medical devices. The commission also recommends requirements ensuring that the AI systems are "robust and accurate, or at least correctly reflect their level of accuracy [, and] … that outcomes are reproducible … and can adequately deal with errors or inconsistencies during all life cycle phases." And it calls for "human oversight" of high-risk AI systems, recognizing that "the appropriate type and degree of human oversight may vary from one case to another."[xxii]

Liability:

The white paper points out that the use of AI technologies may complicate the application of product safety laws when harms occur. Difficulty in identifying whether the AI technology was the cause of the harm, in whole or in part, "in turn may make it difficult for persons having suffered harm to obtain compensation under the current EU and national liability regime." [xxiii]The commission suggests, as a general rule, apportioning liability according to the actor best placed to have addressed the risk of harm, while noting that some of those actors may be located outside the EU.[xxiv] More specifically, it proposes that strict liability be imposed where a product contains defective software or other digital features. It also invites comment on the possibility of reversing the burden of proof, so that a plaintiff would not be responsible for proving the chain of causation when a product relying on AI applications malfunctions.

RECOMMENDATIONS

Thus, as we can see above how EU has specifically drafted a white paper aligning all the possible regulatory aspects of AI in health care under a single policy approach covering

necessary integration for protection. Similarly, in India there is a need of a more comprehensive legal framework of checks and balances, which must be developed to ensure compliance so that the benefits of medical. Since, as of now we don't have single policy formulation with respect to the vision of AI and its possible legal regulatory issues. It is the time for the Indian lawmakers and the judiciary to step in and pave the way for a successful transition of India's healthcare sector into the age of artificial intelligence and solve India's complex healthcare problems. Some of the feasible and practical recommendations in this regard are as follows:

Feasible Alternatives:

1. **Setting up a dedicated regulatory framework to oversee AI in India:**

At present there is no regulatory oversight in this area, and there are fears that over-regulation could lead to a stifling of innovation. This calls for a national-level regulatory agency that oversees developments in AI in addition to formulating a framework that ensures transparency and accountability of AI systems while promoting and enabling innovation. Something in line of European Union can be adopted.

2. **Design standards and appropriate certification system for health systems driven by AI:**

Proof of a clinical trial appears to be the most common certification system asked for by hospitals and other practitioners when considering an AI solution. Yet clinical trials are not tailored for AI technologies and are cost and time intensive. An appropriate certification system is needed to qualify the security and quality of health systems driven by AI. Such a system can incentivise developers to meet needed standards and can work to build trust amongst health practitioners and patients. Design standards are also needed to encourage the development of 'responsible AI' guiding principles to encourage "responsible AI".[xxv]

3. **Liability Framework:**

Predictive AI currently faces limitations in the form of high costs and questions around liability. These can be addressed through understanding the cost vs. quality of care vs. insurability and access. The limitation of liability as described in the IT Act, 2000 may also be unfit to operate

ISSN: 2581 4095
VOLUME 6 – 2020

in the era of artificial intelligence. Section 79 of the Act suggests that intermediary service providers in the field of information technology are merely the carriers of content.[xxvi] Barring exceptions, under Section 79, they would not be held liable for the substance of the content.[xxvii] This rule may have to be re-examined with the implementation of AI systems that are devised by the carriers. Similarly, one of the issues is that the traditional tort law concept of "foreseeability" may not work when AI systems perform a medical diagnosis and treatment. For an individual to be held liable for negligence, the damage that occurred must be ordinarily foreseeable.[xxviii] However, AI or machine learning systems are supposed to learn from the past data and patterns and may behave in ways that the AI developers and designers may not be able to foresee reasonably. The concept of Principle& Agent can be used but still in case of an Artificial Intelligence is bit complex to define who exactly the principle is. Thus, there is a need to create an exclusive liability fixation measure with respect to use of Artificial Intelligence.

4. Emphasize Privacy and Security:

The Supreme Court of India in *Justice K.S.Puttaswamy (Retd.) v. Union of India*[xxix] upheld that privacy is a fundamental right, which is entrenched in Article 21 i.e. Right to Life &Liberty of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2019. However, presently the Information Technology Act, 2000 contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically). The Bill proposes provides for breach notification mandatory. Further, any data breach then would be punishable with a fine and could also attract an imprisonment of up to five years. The Bill proposes the legislative inclusion of the right to be forgotten. Individuals would then be able to limit, delete, delink, or correct any information about him which is misleading, embarrassing, and irrelevant. The Bill states that a data subject has a right to prevent the data fiduciary from using such data or information if data disclosure is no longer necessary, the consent to use data has been withdrawn or if data is being used contrary to the provisions of the law.[xxx] But still issue such as protection of Sensitive Personal Data is yet to be well defined and formulated.[xxxi] The collection and storage of health related data and the potential for bias to be reproduced through the technology raises privacy and security concerns. A key step towards ensuring privacy and

security is for India is to enact and effectively enforce comprehensive privacy legislation as soon as possible.

CONCLUSION

As, we can't deny the importance of technology in the health care sector and especially in a scenario where we can very well understand how critical and crucial is health and should always be given the first priority. But along with the advancement of technology in the health care sector we can't overlook role of the rule of law, human rights, diversity, and fairness, as well as other societal and democratic values in the design of Artificial Intelligence systems and devices with respect to Health Care. Since, this regulatory need is just not a formality rather a very prominent responsibility. Hence, the role of state in identifying the various loopholes and securing them via proper legislative regulations and rules is of outmost importance. To implement and protect these values, Artificial Intelligence systems should also include appropriate safeguards, such as enabling human intervention where necessary. This also means that systems should incorporate a reasonable amount of transparency and responsible disclosure mechanism that allow medical practitioners, patients, and their relatives to understand Artificial Intelligence based outcomes.

Further, to promote responsible stewardship of trustworthy and secure the technological advancement, as well as a fair transition from traditional healthcare, it will be vital that governments work together across border and sectors. Such international collaboration should also extend to the education of medical practitioners, healthcare providers, patients, and other stakeholders to increase their understanding of Artificial based Intelligence and the associated advantages, risks, and limitations of it.

ENDNOTES

[i] T Davenport , R Kalakota , The potential for artificial intelligence in healthcare. *Future Health Journal*, 2019;6(2):94-98. doi:10.7861/futurehosp.6-2-94

[ii]Global Healthcare Artificial Intelligence Market Report, (Available at: https://www.maximizemarketresearch.com/market-report/global-healthcare-artificial-intelligence-market/9847/, last accessed on 27th July 2020 at 11:34PM)

[iii] Ibid.

[iv] Timo Minssen, Sara Gerke, Mateo Aboy, Nicholson Price, Glenn Cohen, Regulatory responses to medical machine learning, *Journal of Law and the Biosciences*, ,11th April ,2020 lsaa002,(Available at: https://doi.org/10.1093/jlb/lsaa002,last accessed on 15th June 2020 at 12:47PM)

[v] Yesha Paul, Elonnai Hickok, Amber Sinha, Udbhav Tiwari, Artificial Intelligence in the Healthcare Industry in India, The Centre for Internet and Society, India Report (Available at: https://cis-india.org/internet-governance/files/ai-and-healtchare-report, last accessed on 15th June 2020 at 02:02PM)

[vi] Natasha Nayak & Rajnish Gupta, Worldwide: Regulating Artificial Intelligence, Mondaq Article (Available at:https://www.mondaq.com/india/new-technology/914028/regulating-artificial-intelligence, last accessed on 18th July 2020 at 01:34PM)

[vii] *Ibid.*

[viii] Pallavi Gupta, Artificial Intelligence: Legal Challenge in India. Heb-Cass, May 2019 – Vol. 3, Issue- 1, Addendum

[ix] Shreya Shenolikar and Darren Punnen, India: Medical Device And Healthcare Year-End Wrap [Part II]: Setting The Stage For An Eventful 2020,Mondaq Article (Available at: https://www.mondaq.com/india/healthcare/887166/medical-device-and-healthcare-year-end-wrap-part-ii-setting-the-stage-for-an-eventful-2020, last accessed on 17th July 2020 at 02:15PM)

[x] E-Health In India, Legal, Regulatory and Tax Overview Nisith Desai Associates ,February 2017 (Available at: http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/e-Health-in-India.pdf, last accessed on 16th June 2020 at 03:15PM)

[xi] Intermediaries, users and the law – Analysing intermediary liability and the IT Rules, Software Freedom Law Centre Report, Available at: https://sflc.in/sites/default/files/wp-content/uploads/2012/07/eBook-IT-Rules.pdf, last accessed on 19th July 2020 at 05:12PM)

[xii] Rajeev Kumar & Pankaj Musyuni,India :Digital Health 2020 ,11th March 2020, Mondaq Online Article (Available at :https://www.mondaq.com/india/healthcare/902762/digital-health-2020, last accessed on 18th June 2020 at 09:19PM)

[xiii] Srivastava SK. Adoption of Electronic Health Records: A Roadmap for India. *Healthc Inform Res*. 2016;22(4):261-269. doi:10.4258/hir.2016.22.4.261

[xiv] *Ibid.*

[xv] *Supra* f.n.7

[xvi] Dr.Milind Antani , Darren Punnen & Anay Shukla, India: DISHA: The First Step Towards Securing Patient Health Data In India, Mondaq Online Article, 3rd August 2018 (Available at: https://www.mondaq.com/india/healthcare/723960/disha-the-first-step-towards-securing-patient-health-data-in-india, last accessed on 18th June 2020 at 10:11PM)

[xvii] *Ibid.*

[xviii] Glenn Cohen, Theodoros Evgeniou, Sara Gerke & Timo Minssen, The European artificial intelligence strategy: implications and challenges for digital health, The Lancet Digital Health Journal VOLUME 2, ISSUE 7, E376-E379, JULY 01, 2020

[xix] The EU's White Paper on AI: A Thoughtful and Balanced Way Forward Lawfare Blog,(Available at: https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward, last accessed on 27th July 2020 at 01:06AM)

[xx] White Paper on Artificial Intelligence A European approach to excellence and trust, European Commission White Paper (Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, last accessed on 27th July 2020 at 01:16AM)

[xxi] *Ibid*

[xxii] *Ibid*

[xxiii] Supra fn. 20

[xxiv] *Ibid.*
[xxv] *Supra* f.n. 2.
[xxvi] Malvika Kapil Kalra, Intermediary Liability under the Information Technology Act: Time for an Amendment? Bar & Bench (Available at: https://www.barandbench.com/columns/intermediary-liability-under-the-information-technology-act-time-for-an-amendment, last accessed on 19th July 2020 at 03:49PM)
[xxvii] The Future is here: Artificial Intelligence and Robotics, Legal, Regulatory and Tax Overview Nisith Desai Associates ,May 2018 (Available at: http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Artificial_Intelligence_and_Robotics.pdf, last accessed on 20th June 2020 at 04:16PM)
[xxviii] *Supra* f.n. 8
[xxix] *Justice K.S.Puttaswamy (Retd.) v. Union of India* [Writ Petition No. 494/ 2012]
[xxx] Vinod Joseph & Protiti Basu, India: Right Of Erasure - Under The Personal Data Protection Bill 2019,Mondaq Article (Available at: https://www.mondaq.com/india/data-protection/877732/right-of-erasure--under-the-personal-data-protection-bill-2019, last accessed on 20th June 2020 at 12:39PM)
[xxxi] Mohan Dewan, Personal Data Protection Laws in India, 13th May 2020 , R.K. Dewan & Co. (Available at: https://www.rkdewan.com/articledetails.php?artid=183, last accessed on 19th June 2020 at 01:11PM)