Vol. 13 No. 1 ISSN: 0976-3570

Artificial Intelligence, Big Data and Health Privacy: Need for Democratization and Regulation in Health Data Processing System

Tridipa Sehanobis[1]

Abstract

The paper seeks to depict the present status of Artificial Intelligence ("AI") in the healthcare system of India and its issues relating to data privacy. AI is being a major contributor to health and medical domain not only increase its efficiency but also to gain economic firmness in these sectors in India. Owing to this, comes deep concern on its regulation and law limits while using the personal data of the patients for any other purposes than treatment. The use of AI which entails constant exchange of information and data between the patient and the AI service providers, raises serious concern for data privacy, as they are using the sensitive personal data of the individuals for other purposes like prospective trainings, creating algorithms, advertisement, etc. Hence, with big datasets there is associated serious threat and challenges to the privacy of the individuals, which is required to be addressed. This is possible with the foremost step of the democratization of health data and healthcare where individual will have better access to his/her health information and therefore manage their own health. This can further be implemented through the usage of AI-based technologies, like wearable bands, glucometers, etc. following a due process. Again, the operators of these devices should be strictly regulated through certain regulation and legislation such as Data Protection Bill, which safeguards the privacy of the data owners. The legislature should ensure the passage of the laws following due process, discussion and participation of the people to ensure inclusivity and safeguard the interest of each individual. The paper tries to suggest measures to make use of AI in healthcare ecosystem in a regulated manner so that its use is more of importance than of controversy.

Keywords: *Big Dataset, Sensitive Personal Data, Health Data Privacy, Artificial Intelligence, Surveillance Capitalism, Democratization, Due Process*

[1] Assistant Professor, Indian Institute of Legal Studies, Siliguri, West Bengal, India and Research Scholar, Rajiv Gandhi National University of Law, Punjab, India.

I. Introduction

"The Fourth Industrial Revolution, finally, will change not only what we do but also who we are. It will affect our identity and all the issues associated with it: our sense of privacy, our notions of ownership, our consumption patterns, the time we devote to work and leisure, and how we develop our careers, cultivate our skills, meet people, and nurture relationships."[2]

-Klaus Schwab

With the developments in Artificial intelligence our world has drastically transformed in every aspect. John McCarthy, first devised the term "Artificial Intelligence" ("AI") and defined it as, the "science and engineering of making intelligent machines."[3] AI can also be described as when a machine that retains the capacity of aptitude as that of a human. These AI technologies require a collection of huge data and information related to the specific subject, it is working on, so as to builds up the requisite ability of decision making. On the other hand, it is to be remembered that, the software developers who develops the AI, possess the control over these mechanisms, the data stored in them, including its action and reaction.

In the present-day digitalized world, the dependence on technology is inevitable, that leads to stockpiling of massive personal data termed as 'digital data', which in turn is used by the AI device for upgrading the standard of living. Consequently, all our personal data ranging from our preferences, to daily personal interactions, to medical reports, to specific symptoms and habits, etc. are gathered, stored, treated, and profiled by AI technologies, which are then used for various purposes such as for certain commercial, development, training and advertisement drives. This particular process of gathering data and its subsequent usage overruns the individual's privacy, confidentiality and informed consent. The application of the system of AI in healthcare sector is though undoubtedly helpful and largely contributing to the serve the people thereby adding up to the strength of doctors; but its application has also been a serious threat to the individual's privacy.

AI in health care system largely relies on the individuals' health information, which they have shared voluntarily or involuntarily with the health care

[2] J. J. Peila, Supporting Student Transitions: Integrating Life Design, Career Construction, Happenstance, and Hope, 30 S. Afr. J. High. Educ., 54, 55 (2016).

[3] John McCarthy, What Is Artificial Intelligence? Stanford University, (Jul. 19, 2020, 09:20 PM), http://www-formal.stanford.edu/jmc/whatisai.pdf.

agencies including doctors, hospitals, clinics, laboratories, etc. All these agencies carry out their functions with the help of new media technologies. They have created their own databases in order to store the patients' information. The computer network and internet communication technologies also allow the patients to access their health reports at any place in the world. Patients using the new media devices may interact with the foreign doctors, and share their test reports. In the realm of new digital era the labs of diagnosis and prognosis have become extremely efficient, helping the patients to opt for proper treatments. Besides, the contemporary AI enabled wearable fitness bands and mobile applications have added up to the potentiality of the digitalized world to make paths in diagnosis and prognosis. The individuals use health apps and wear the trendy fitness bands that measure their heart beats, calories, location, and physical activities and so on. Everything is being stored online forming hefty database of the same. In this way AI has an unprecedented access to all these databases.

However, it cannot be forgotten that the information related to the individuals' health though shared voluntarily is sensitive in nature, for the techniques of medical tests are capable in discovering the present and future diseases, and of tracing the genetic traits attached with the particular race, caste, ethnicity or religion. For example, the Artificial Intelligence may predict that a person has Parkinson's disease based on the data stored on the computer network and if this data is shared or used for some unauthorized purpose, it would lead to severe breach of his or her privacy. The concerned individual has every right to prohibit the AI agents from disclosing such information to anyone. Individuals do have reasonable expectation of privacy that their shared information should be kept confidential for various reasons.

II. Importance of Health Privacy

The healthcare data of the patients includes a number of sensitive information ranging from his/her age to sleeping habits to personal food habits or addictions to sexual life to symptoms of peculiar diseases and so on. These data along with it carry the personal identifiable of the patients as well. Now these information of different patients are stored and maintained in digitalized mode for efficient management and prompt retrieval of the dataset thereby to enhance the healthcare delivery. Healthcare data can be used by and shared with different stakeholders of the healthcare system for providing effective treatment, such as:

- It can be shared with the clinical co-workers by the concerned doctor to provide the required standard of care and to ensure clinical or medical care coverage
- It can be used by the laboratories and scanning/x-ray centers so as to decide if the results relating to the condition of the patient are within the standard parameters or not and for research and clinical trials as well.
- The Medicine companies may also require the patient's health dataset for clinical trials or for discovery of required essential drugs.
- Even the medical insurance firms need the access to such data toverify whether the details given the customer were correctly stated or not based on which the level of insurance coverage has been offered and whether the company may suffer any loss for the said customer or not.

Based on all these purposes the healthcare dataset of the individuals moves from one place to another and different stakeholder have access to this information. However, it is to be remembered that personal identifiable data should be preserved adopting highest security and confidential standards because healthcare data being the personal sensitive data of the individuals are subject to privacy and security regulations.

A. Privacy Values

'Privacy' is experienced on a subjective level and commonly perceived differently by different people.[4] In contemporary times, the word is used to indicate different, but intersecting, concepts viz., the right to bodily integrity or right to be free from invasive search or reconnaissance, right to human dignity, right to personality and self-development and so on. The concept of 'privacy' is wide and connotes within its ambit right to have control over the bodily and psychological conditions. Nobody has right to intrude into one's mind or psychological thoughts and conditions and all the data relating to it belongs to the person alone. Constitutionalism provides protection against such intrusion even if the intruder has the technological capability to read the minds of the individuals.

[4] William W. Lowrance, Privacy and health research: A report to the U.S. Secretary of Health and Human Services. 1997, (Jan 18, 2021, 3:31 PM), http://aspe .hhs.gov/DATACNCL/PHR.htm.

Collste contends that the notion of 'privacy' is basically grounded on three universal fundamental ideals viz., 'autonomy', 'freedom', and 'personal relationships'.[5] Accordingly, respecting these fundamental values will itself amount to respect for 'privacy', as privacy is an essential pre-requisite for realizing those values. Even though cultural and social norms of individuals may differ with regard to the extent to which privacy has to be protected in order to achieve those fundamental values, but such changes do not reflect a profound ethnic variance in the notion of 'privacy' in itself.

B. Importance of Health Privacy to Enjoy One's Right to Personality

The paradigm of privacy is utterly broad and it rightly determines the question as to who would have access to personal information of an individual and under what circumstances. As far as health data privacy is concerned, it includes the aspect of gathering, storing, and using of personal information of the individuals and scrutinizes if such information could be collected primarily and also to examine the justification based on which information gathered for one purpose can be handed down for another purpose. Maintaining and safeguarding the privacy of the patients is regarded as the foremost principle in the ethical and just medical care and research. A higher degree of privacy protection is expected when it comes to health data as it includes, various sensitive information relating to the individual that is essential to one's personal development. Health data as mentioned above contains various facets of the individual life ranging from age to sexuality to major abnormalities and diseases and so on.

For whatsoever purpose the heath data of an individual is to be used, be it for improvement of the diagnostic methods, discovering new methods of treatment or for medical research or other legalized purpose, taking its due care and caution while using it is indispensable. If such data is not handled with due care and protection, it can inexorably cause major damage to the individual personality among everyone because slip of any such data, to an inappropriate person or for any un-consented secondary purpose can unwarrantedly cause harm to the individual's human dignity, self-confidence, and personality to a great extent. Such data may have adversarial repercussions on that individual's reputation, reliability, confidence in his or her workplace or family or in the society as a whole. For example, if an employed individual has severe heart disease for which he may at any time be in a serious condition (life-

[5] Goran Collste, Global ICT-ethics: The Case of Privacy, 6 JICES., 76, 79, (2008).

threatening), he may not be preferred to hold any higher position in office on basis of such information. As this information raises question on his efficiency which is crucial with respect to a higher position.

C. Role of AI in Improving Healthcare Delivery by Using Personal Health Data

Deep learning, a subcategory of machine learning related to the domain of AI, is remarkably known for its adeptness in training potent algorithms for the grouping of medical pictures and other high-dimensional data.[6] Altogether, these methods may provide for various benefits for patients, who are consumers, which include automatic screening and prioritizing of disease and effective treatment plans. For instance, AI supports in detection of diabetic retinopathy, retinopathy of prematureness, and glaucoma which could advance early discovery and treatment.[7] Besides, AI is used for prediction of future diseases and its possibilities, such as, critical kidney injury to age-related macular strength deterioration and diabetic retinopathy; in the future, such predictive AI would result for betterment in precautionary treatment plans.[8] At the same time, AI can facilitate health research by effectively managing dataset of the individual for diagnosis of the disease. This paves the way to figure out the pattern of the diseases and to trace the symptoms, based on which the medical research can effectively take place. This further benefits the individuals, such as, it enables access to new treatments, improved diagnostic methods, and more active ways to avert diseases and deliver proper care and remedy.

Public Use

Big data empowers more accurate and efficient assessments of health care quality and efficacy, which can promote treatment optimization. Big data can

[6] Yuka Kiharaet. al., Estimating Retinal Sensitivity Using Optical Coherence Tomography with Deep-Learning Algorithms in Macular Telangiectasia Type2, Jama Network Open, (Jul. 19, 2020, 09:50 PM), doi:10.1001/jamanetworkopen.2018.8029.

[7] Hanruo Liu, et. al., Development and Validation of a Deep Learning System to Detect Glaucomatous Optic Neuropathy Using Fundus Photographs, 137JAMA Ophthalmol, 1353, 1355 (2019).

[8] FilippoArcadu, et.al., Deep Learning Algorithm Predicts Diabetic Retinopathy Progression in Individual Patients, 2NPJ Digit Med, 92, 95 (2019).

help to improve the quality of service delivered by the hospitals,[9] to formulate scientific hypotheses,[10] to compare the usefulness and success of different involvements, and to monitor drug and device safety. The AI is benefiting heath care sector by executing cognitive technology to unwind a huge amount of medical record and to facilitate in effective diagnosis. For example, Nuance, a product service provider, uses AI and machine learning for predicting the intent of particular individual. Its products are used in the healthcare sectors, which basically helps in storing, collecting and reformatting data for enabling consistent and faster access to all medical data of the patients, and to learn the behavioral pattern of the patients, in order to analyze or diagnose more efficiently.

The Indian Government is remarkably heading towards digitalizing the healthcare environment in India basically through the deployment of the AI-technologies. In the National Health Policy (2017) the government first codified the shift of the pen-paper based functioning of healthcare system to digitalization. Moreover, the National Digital Health Blueprint (NDHB 2019) advances this prophecy to recognize constituent elements that influence technological foundational en-routing for capacious technological development for diverse purposes and depend in a most elementary way on high data integrity of the health.[11]The government has already made ways in digitalizing the medical records of the patients through the system of Electronic Health Record (EHR). However, the EHR system lacks behind somehow in public health organizations for its high rate in its application and for extraordinary burden on clinicians owed to cumbrous input and maintenance actions.[12]

[9]Hospital Inpatient Quality Reporting Program, Centers for Medicare and Medicaid Services, (Apr. 30, 2021, 05:15 PM) https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/HospitalQualityInits/HospitalRHQDAPU.html.

[10]Issac S. Kohane, Using Electronic Health Records to Drive Discovery in Disease Genomics, 12 Nat Rev Gent. 417, 421 (2011).

[11] Final Report on National Digital Health Blueprint (NDHB), Ministry of Health and Family Welfare (MoHFW), Government of India, October 2019 (May 23, 2021, 05:15 PM), https://main.mohfw.gov.in/newshighlights/final-report-national-digital-health-blueprint-ndhb.

[12] Rashmi Mabiyan, India Bullish on AI in Healthcare without Electronic Health Records, ETHealthWorld, (May 24, 2021, 08:10 AM), https://health.economictimes.indiatimes.com/news/health-it/india-bullish-on-ai-in-healthcare-without-ehr/73118990.

However, in 2019 the Health Minister of India had promised to prioritize AI in the healthcare to address such gaps.

Where doctor-patient ratio stands to 1:10,189, call for technological application is inevitable to meet efficient healthcare delivery. For instance, an AI-based breast cancer detecting device that uses a non-invasive, economic resolution based on heat-mapping for primary recognition of breast cancer has been able to notice breast cancer up to five years earlier than a mammography with reduced reliance on trained technicians.[13]Following such benefits and efficiency that would arise from these AI-technologies various states in India have undertaken to embrace this wide implementation of it in the healthcare ecosystem. The state of Telangana for instance, has stated 2020 as the 'year of AI', with the objective of promoting AI-enabled inventions across e-governance, cultivation, healthcare and education.[14]Some of the ingenuities assumed by the central government to ensure the application of AI technologies in public health sector are: Imaging Biobank for Cancer by a collaborative effort of the NITI Aayog and Department of Bio-Technology (DBT).This targets to form a database of cancer associated radiology and pathology images of more than 20,000 profiles of cancer patients focusing on major cancers predominant in India.[15]This will form an extensive database of the cancer patients including their patterns, habits, and peculiar symptoms which data will further stored and processed for future analysis and treatment purpose.

Private Use

The private healthcare sector in India has also widely deployed AI, to advance the proficiency of the healthcare delivery system and to serve its patients more proficiently. For example, IBM Watson is installed in Manipal Hospitals for diagnosis and treatment of various kinds of cancers. IBM Watson for Oncology combines deep proficiency of the leading oncologists in cancer care with the

[13] Sudip Bhattacharya et al., Artificial intelligence enabled healthcare: A Hype, Hope or Harm, 8(11) J Family Med Prim Care, 3461, 3462 (2019).

[14]AI Technology to Bloom in Telangana, The Hindu, (Apr. 09, 2021, 05:34 PM), https://www.thehindu.com/news/cities/Hyderabad/ai-technology-to-bloom-in-telangana/article30464412.ece.

[15]Health Ministry to use Artificial Intelligence in safe way in public health, The Economic Times, (Apr. 11, 2021, 04:30 PM), https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/health-ministry-to-use-artificial-intelligence-in-safe-way-in-public-health/articleshow/70189259.cms?from=mdr.

IBM Watson's speed to help the clinicians, for considering the individualized cancer treatments for their patients.[16]Currently, the Aravind Eye Care Systems is working in collaboration with Google Brain, which formerly helped Google to produce its retinal screening system by contribution of images which in turn aided in training process of its image analyzing algorithms.

Apart from the superior companies, like Google and IBM, India has hosted many startup companies as well that focus being on AI mainly to detect disease. For instance, Niramai Health Analytix implements thermal analytics for detection of breast cancer at initial stage, while Advenio Tecnosys discovers TB from chest x-rays images and severe contagions from ultrasound images.[17]Again, BeatO, a startup established in India in 2015, launched an app enabled with glucometer, that can be plugged into a smartphone for screening and to keep the reading saved in the app. This can be retrieved at any time for further assistance and meeting any emergency situation.

Most importantly, the wearable fitness equipment which are most popular among the masses nowadays, are storing up huge amount of personal data on daily basis in lieu of various social and medical benefits. Wearable fitness devices largely embrace a wide variety of technologies including mobile health (mHealth) technology.[18]By and large the MHealth technologies have the competence "to improve the quality of health care and reduce medical errors; to reduce the cost of health care; and to increase access to care by democratizing and demystifying medicine."[19]Medical device startup named ten3T produces medical wearable devices, and its invention was Cicer, a palm-sized patch sticker with multiple embedded sensors.[20]These devices keep track of the day to day activities of the individuals, storing all the data time to time which retrievable at any time later for keeping record of the health trends. This data

[16]Artificial Intelligence in Medicine, IBM Watson Health, (Apr. 10, 2020, 06:30 PM) https://www.ibm.com/watson-health/learn/artificial-intelligence-medicine.

[17] Artificial Intelligence in the Healthcare Industry in India, cis-india.org, (Jul. 25, 2020, 07:54 PM), https://cis-india.org/internet-governance/ai-and-healthcare-report.

[18] Mhealth: New Horizons For Health Through Mobile Technologies, WHO, 3 Global Observatory For Ehealth Series, (Mar. 11, 2021, 07:32 AM) http://www.who.int/goe/publications/goe_mhealth_web.pdf.

[19]Nathan Cortez, The Mobile Health Revolution?, 47 U.C. DAVIS L. REV. 1173, 1176 (2014).

[20]Artificial Intelligence in the Healthcare Industry in India, cis-india.org, (Jul. 25, 2020, 07:54 PM), https://cis-india.org/internet-governance/ai-and-healthcare-report..

can inform doctors of associative health pattern, for instance, the correlation among exercise and pattern of sleeping habit, and association between particular place and the existence of weight-related diseases, on a local or national scale.[21]

These technologies aid in the early discovery and prevention of health issues while transportation, and even at home as well. Similarly, with the usage of wearable fitness devices the costs of health care may also be reduced as the use of such technologies certainly reduce the number of visits to doctors. The blend of big database and AI thus provides many prospective benefits for healthcare systems that increase efficiency with less expenditure.

III. Threats of Artificial Big Data on Health Privacy

The gradual emergence of erudite AI system and the collaboration of many knowhows like the AI, the Internet of Things (IoT), and the Internet of Living Things (IoLT) acts as a stern risk to our privacy. Though there are ample of benefits derived out of the implementation of AI in the healthcare sector, number of ethical issues emerges out of it due to lack of regulation regarding its usage and control. One of the concerns is that of data privacy issues, which arises with the implementation of AI. This leads to trepidations regarding the steadiness between inventions and privacy and the need for effective protection of data privacy mechanism that can be developed sideways with AI implementation.

As it is known that for the purpose of machine learning and deep learning, a huge amount of data is required to accomplish its necessity for advancement and testing- this may be perceived as one of the major drawback of AI mechanism. Furthermore, with the help of AI-enabled healthcare devices the government, the corporates and the individuals are able to make use of the personal data processed and stored by these technologies to show the statistical inferences,[22] such as physical traits, race, credit merits, insurance risk, employment or academic ability and so on. Although apparently, it is the anonymized data of the patients that are used for technological development, but there exist certain risk. The value of generosity entails that healthcare service providers “do no harm”; however, violation of patient’s privacy can

[21] Dolezal BA et al., Interrelationship between Sleep and Exercise: A Systematic Review, 2017 Adv Prev Med, (2017).

[22] Nicolas P. Terry, Big Data Proxies and Health Privacy Exceptionalism, 24 Health Matrix 65, 77 (2014).

result into serious damages and can also cause unintentional results, which can possibly have a negative impact on one's occupation or insurance coverage[23] and may also permit cyber attackers to get Social Security figures and individual economic data.[24]

Increasingly, generating anonymous data and removing identifiable information from big database can be a formidable job. Rather, it is very natural that, even with utmost rigorous labors, there will be at least a potential threat of re-identification.[25] This risk is very much associated with ophthalmology. But that is not the only area, because it is now possible to implement facial identification software system to three-dimensional reformation of computed imaging of the head. Moreover, specific characteristic from the periocular region is used to recognize the patients' age by means of machine learning algorithms.[26] From fundus images even, gender, age, and cardiovascular risk factors can be recognized.[27] The data which is not even a medical image have the potential to recognize individual by its connection with other information as the patients' data adds on over time.

So, in the rung of advancement, we are losing our privacy to a large extent, remedying which is a mere attempt. As rightly explained by Christina P. Moniodis that,

> "The creation of new knowledge complicates data privacy law as it involves information the individual did not possess and could not disclose, knowingly or otherwise. In addition, as our state becomes an 'information state' through increasing reliance on information – such that information is described as the 'lifeblood' that sustains political, social, and business decisions. It becomes impossible to conceptualize all of the possible uses of information and resulting harms. Such a situation poses a challenge for courts

[23] Price WN, et. al., Privacy In The Age Of Medical Big Data, 25Nat Med., 37(2019)

[24] M Shi, et. al., A Privacy Protection Method For Health Care Big Data Management Based On Risk Access Control, 23Health Care Manag Sci., 1, 9 (2019).

[25] Luc Rocher, et.al., Estimating The Success Of Re-Identifications In Incomplete Datasets Using Generative Models, 10 Nat Commun., 3069 (2019).

[26] Kishore Kumar Kamarajugadda and Trinatha R. Polipalli, Extract Features from Periocular Region To Identify The Age Using Machine Learning Algorithms, 43 J Med Syst., 196, 197 (2019).

[27] Ryan Poplin, et. al., Prediction of Cardiovascular Risk Factors From Retinal Fundus Photographs Via Deep Learning 2 Nat Biomed Eng., 158, 160 (2018).

> who are effectively asked to anticipate and remedy invisible, evolving harms."[28]

In spite of certain privacy and security concerns attached with the implementation of AI, countries and governments around the world are evolving and innovating AI technologies and investing for its development. In 2018, India has actively recognized the use of AI expertise in various fields from healthcare to crime prediction to education, by the National Strategy for Artificial Intelligence that authorized NITI Aayog to launch national program on AI[29] and the Report of the AI Task Force. The usage AI mechanism is entangled with every aspect of human life ranging from its finance, physical traits, genome, faces, emotions, environment, culture and religion as well, which adds up to the issue of data protection and privacy concern.

A. Abuse of Health Data by Totalitarian Governments

The data protection serves many personal, psychological and social functions of right to privacy. An individual seeks protection to his or her health information when there is an apprehension that the information can be made subject of his or her discrimination, embarrassment or harassment. The exploiters of the health information could be anyone. It may be close on or foe. The disclosure of the information can appease those who have curiosity to know everything about others and to make idle gossips. Moreover, the health information can also be abused by the totalitarian regimes like Nazi regime. Adolf Hitler's idea to create pure race is a serious violation of the inclusive societies. The arrogant rulers have their own definition about healthy or unhealthy persons; consider the unhealthy ones as a liability on the so-called perfect society. The autocratic governments do discriminate their citizenry on the basis of race, gender, sexual orientation, etc.

Several governments have been benefitted by the advancement of AI, improved IoT and IoLT. For example, the use of Portable genome sequencer MinION and Metrichor which uses AI technology in epidemiology[30], aids in predicting the risk of diseases. Another instance is, Sequenom Inc., using

---

[28] Christina P. Moniodis, Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy, 15 (1) Yale Journal of Law and Technology, 141,153 (2012).

[29] National Strategy on Artificial Intelligence, NITI Aayog, (Jul. 24, 2020, 08:44 PM), https://niti.gov.in/national-strategy-artificial-intelligence.

[30] HengyunLu, et.al., Oxford NanoporeMinION Sequencing and Genome Assembly, Science Direct (Jul. 23, 2020, 03:45 PM), https://doi.org/10.1016/j.gpb.2016.05.004.

AI, that interprets genetic code into pertinent data. Government and other regulatory bodies, on the basis of these data generated by AI make learned decision to tackle and control the spread of maladies and to avert epidemics.

But what if the government itself has a distorted motive to accomplish by these data. Incident like prosecution of religious minorities is widely practiced worldwide, particularly in Africa and Asia. They are subject to ethnic cleansing in their regions. Their identities are now stateless persons or refugees. Social taboos are lynching the individuals having sexual orientation which is not in consonance with the majority opinion. It is apt to mention the fact that the unprecedented capabilities of the new media technologies and AI mechanism can disclose all these factors to such types of governments. By relating the genetic traits and other physical traits with the help of artificial intelligence, the discriminatory governments may achieve their political gains. In K.S. Puttaswamy v. Union of India,[31] the court explicitly held that the ambit of data protection safeguards 'principle of non-discrimination' thereby ensuring that the pooling of data should be in such manner as not to show prejudice on the ground of race, or ethnic origin, or political affiliation, or spiritual views, or heredity or health status or sexual orientation.

B. Surveillance Capitalism by Big Corporates

Increasingly, the private companies are deeply interested in the individuals' health information. A rising number of employers by means of fitness devices encourage corporate wellness so as to "create [a] culture of well-being", "improve participant health status", "increase employee productivity," and "boost acquisition and retention."[32] Big data on health information has the potential to empower the controllers to act in biasness. This notion can be best explained by the concept of "Surveillance Capitalism. According to Sushna Zuboff "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary behavioural surplus, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into prediction products that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace that I call behavioural futures

[31] K.S.Puttaswamyv. U.O.I, AIR 4161 (SC: 2017).

[32] Howell, Kathryn et al., 7 Reasons to Invest in Well-Being, 2015 Psychology of Violence (2015).

markets."[33] 'Surveillance capitalists have grown-up enormously rich by these trading processes, as many corporates are keen to lay bets on our future consumer behaviors.

In surveillance capitalism, the commodities for sell are the personal data of the individuals or the consumers, and the generation and production of this information is made by mass surveillance on internet. The consumers' behaviors are learned and thoroughly analyzed by such surveillance and stored specifically to influence our further behavior. Here the role of frightful five those are, Google, Facebook, Amazon, Microsoft, Apple, is noteworthy. They shop our behavior and experiences with the help of technological advancement like AI. Thereafter, they encash by selling these personal data of the consumer to third-party companies. Such data can be major factor for making wealth by attacking the consumer with advertisements, or for taking major decision which can be detrimental to the interest of the consumer thereby infringing his or her privacy. For example, now-a-days whenever we are facing trouble with our health, there is a tendency to search for the remedy at hand. Hence, we search in the internet using our browsers in phone or laptop or sometimes by surfing different social media sites. The search history saves our behavior and our concerns which is used by the different browser and social media companies as commodity. Subsequently, whenever we get back to those sites, we are attacked with the remedies that we were looking for, even in those sites where we did not search for such remedy for our health. This is the simple example we encounter every day. This activity reveals that our personal concerns are circulated internally within different companies which get to know our health conditions and information. These sensitive information are further transferred to other third-party companies as assets detrimental to our interests.

Similarly, when we use fitness bands, they keep track of our health status and accumulates all such data to be used as wealth. Even small companies are enchasing on the personal data by such operation. The third party brokers are selling our personal information to the big corporates, thus leading to the accumulation of wealth (personal data) in the hand of online companies.

[33] John Naughton, The Goal is to Automate Us: Welcome to the Age Of Surveillance Capitalism, The Guardian, (Jul. 25, 2020, 08:54 AM) https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

Pharmaceuticals using the artificial intelligence may colonize the health by inventing addictive and de-addictive features of a medicine knowing the preferences and behavior of the consumers by medical diagnosis and online surveillance made by different corporates. Life insurance companies may manipulate the agreements with their clients, and decide the policy unilaterally, by buying personal data of the consumer from other companies. It would be against the social security measures, which are promised under the principles of constitutionalism. This hampers the bargaining power of the patients and the consumers.

Where health information is a valuable asset and wealth for the healthcare service providers, who are abusing it for commercial purposes, hacking of the medical databases gets flourished. Hackers are in the business to track medical history of the individuals including HIV reports. Such an incident took place in 2016, when the hacking of a Mumbai-based diagnostic and test center database led to the disclosure of medical reports (including HIV reports) of about 35,000 patients.[34] This particular database possessed information of patients across India, and many were uninformed that their particulars have been uncovered. Again in K.S. Puttaswamy v. Union of India,[35]the court was of the view that sharing of medical information of an individual without his approval leads to a breach of privacy.

Advertisement, management and sale of the products and services provided by such health care agents depend upon the medical tracks of the individuals. Health related fears and anxieties can be created through the abuses of artificial intelligence. Consumer behavioral patterns let the data controllers to make the opinion among masses. Rumors or fake news make money for the wrongdoers.

IV. Legal Framework Relating to Data Privacy Issues

In order to evade above mentioned wrongdoings, it is necessary that the health related data must be protected from the unauthorized accesses. Right to privacy is a one of the basic rights legally recognized under various international human rights documents. It is also recognized as a part of fundamental right to life and

[34] How is Data Transforming Healthcare in India?, Znetlive Blog, (Jul. 19, 2020, 07:30 AM) https://www.znetlive.com/blog/data-transforming-healthcare-india/.
[35] K.S.Puttaswamy v. U.O.I, AIR 4161 (SC: 2017).

personal liberty under Indian Constitution. Besides, there are number of other laws aiming to recognize and protect the arena individual privacy.

A. International Conventions

At international level, both Universal Declaration on Human Rights[36] and the European Convention on Human Right[37]s recognizes the enforcement of the fundamental right to privacy, reputation, dignity and self-respect. The International Covenant on Civil and Political Rights provides protection to the individuals against unwarranted interference with their privacy.

B. Right to Privacy under the Indian Constitution

Article 21 of the Indian Constitution provides for "Right to Life and Personal Liberty" and the Indian Judiciary has implicitly included Right to Privacy under this right. In K.S. Puttaswamy v. Union of India,[38] the Supreme Court, recognized the right to privacy as a fundamental right under article 21 of the Indian Constitution. The Court categorically held that,

> "Data such as medical information would be a category to which a reasonable expectation of privacy attaches. There may be other data which falls outside the reasonable expectation paradigm. Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual. This is evident from the emphasis in the European data protection regime on the centrality of consent. Related to the issue of consent is the requirement of transparency which requires a disclosure by the data recipient of information pertaining to data transfer and use."

On this ground the court observed that in formulating a data protection regime the State must consider harmonizing the privacy principles along with the other values of data protection keeping in mind the legitimate concerns of the State. During the course of its hearing it was informed by the Ministry of Electronics and Information Technology that they formed a Committee of Experts to identify the major areas of issue relating to data privacy and also to come up with draft legislation. Resultantly the Personal Data Protection Bill, 2018 was tabled in Parliament.

---

[36] UDHR, art. 12.

[37] ECHR, art. 8.

[38] K.S.Puttaswamy v. U.O.I, AIR, 4161 (SC: 2017)

C. Personal Data Protection Bill, 2018 (PDP Bill)

The ministry came up with the Personal Data Protection Bill, 2018 (PDP Bill). It provides for the constitution of a Data Protection Authority in the country. The authority would have power to issue appropriate directions to the data fiduciary and can conduct inquiries with regard to any case of breach of data privacy the data fiduciary.[39] The Bill is made in lines with General Data Protection Regulation (GDPR) and legalizes the handling of personal information of citizens by the government, incorporated companies in India, and foreign companies that are using the personal data of customers in India only on certain grounds explicitly mentioned in the Bill. In essence, the data principals demand that the data controllers should be made responsible for protecting the information of the data subjects. Apart from the obligation that the data of the individuals are collected legally, the collector of such data must also guarantee that personal data of the individuals are not misused or exploited.

Processing of sensitive information is prohibited. Data controllers cannot collect information more than its requirement. The information can be used for the authorized purposes only. While doing so, it is mandatory to take the explicit consent of the data subjects. The Data Protection Bill would be applied on both public and private entities. But the sensitive information collected for the purposes of security of state or preventing commission of crime falls under the exception clause.

Furthermore, the Bill provides for "Right to be Forgotten", which is made available to the data subject, giving him a right to restrict or prevent continuing the data controller from disclosure of his or her personal information.[40] The information should be removed once the purpose is achieved. Recently, in the case of Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.[41] (2019), the Delhi High Court held right to be forgotten as an inherent part of right to privacy under article 21 of the constitution.

---

[39] The Personal Data Protection Bill, Ministry of Electronics and Information Technology, MEITY, GOI, ss. 62 and 64, (2018).

[40] *Id.*at s.27.

[41] Z.A. Khan v. Quintillion Business Media Pvt. Ltd., 175 DRJ, 660, (DHC:2019).

D. Digital Information Security in Healthcare Act

The draft of the Digital Information Security in Healthcare Act ("DISHA") notified by the Ministry of Health & Family welfare in 2018 for public consultation[42], was a big step toward health data protection regulation. This draft Act based the data protection regime on a strict consent mechanism in every stage of data collection and processing. This draft Act is a special law to regulate the area of health data. The remarkable attempt of DISHA is to put a complete ban on the commercialization of the health data. Section 29 (5) of DISHA runs as:

> "Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government."

This is a major quantum leap towards the protection of the medical data regime. Moreover, the draft act also aims to address the concerns associated with the data collection by the healthcare applications and wearable devices which comes under the purview of other entities under this act. The above referred provision of DISHA also applies to them. According this draft act the data collectors are under strict obligation to obtain the consent of the data owner explicitly for every use of the identifiable data for the prescribed used.[43] It is to be noted that the users are at liberty to refuse the consent for data generation, collection or processing at any stage he or she wishes.[44] The Act envisions a holistic approach towards data protection seeking to safeguard the data owner's (principal's) the right to privacy, confidentiality, and security of their digital health data, which may be collected, stored and transmitted according to the provisions of this Act.[45]

---

[42] Digital Information Security in Healthcare Act, F.No Z-18015/23l2017-eGov, Ministry of Health and Family Welfare, GOI, (May 02, 2021, 3:15 PM), https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf

[43] Digital Information Security in Healthcare Act, e-Gov, MHFW, GOI, s. 30 (2) and 29 (2017).

[44] id. At s.28 (2).

[45] id. At s.28 (1).

Interestingly, if both the PDP Bill and DISHA are passed as an Act, it will definitely form a strong data protection regime in India, including the governance of the digital health data. However, a thin line of difference between both the above-mentioned act has been noticed with regard to the consent mechanism. The PDP Bill seeks the requirement of obtaining consent before using this health data by the entity i.e., only at one stage. On the other hand, the DISHA provides stricter provisions and requires obtaining of the consent of the data owner at every stage of data collection from generating to processing to transmission to that of its storage. Nonetheless, the conflicting view can be resolved by giving way to the special act DISHA over the general one PDP Bill, as the DISHA exclusively deals with the regime of Health Data Protection.

But the major concern here is both the act are yet to be passed by the Parliament. So, at present they are not at operation. Nevertheless, there are various existing provisions of laws and rules that deal with the data protection and privacy concerns of personal data. The relevant existing laws are discussed below:

E. The Consumer Protection Act, 2019:

The issue relating to sharing of personal data without informed consensus of the data principal can be addressed under the provision of this Consumer Protection Act, 2019. The Act makes a provision of "unfair contract" means any contract that takes place between a manufacturer or service provider or trader on one side and the consumer on the other side, which contains such terms and conditions that will have serious impact on the rights of such consumer. Such contract may include, authorizing one party to assign the contract to the disadvantage of the consumer, lacking his consent; or imposing on the consumer any arbitrary charge, responsibility or condition which is prejudicial to the consumer.[46] Thus the contract that the various corporates, having the control over that data of the individuals, make with other companies, to share such personal information without informed consent, acts in detriment to the interest of the individual consumer. Therefore, this can be categorized under "unfair contract" under this act.

[46]The Consumer Protection Act, The Gazette of India, s. 2(46) (2019).

F. Information Technology Act, 2000

In explicit sense, it is only the Information Technology Act, 2000 that provides for the matters connecting to data privacy, payment of compensation and imprisonment in case of unauthorized exposure and ill use of personal data and breach of agreed terms with regard to personal data. The act provides that a body corporate should be very careful, which is in possession of, and dealing or handling any sensitive personal data or information, otherwise any negligence if observed in its part in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, would make that corporate liable to pay damages to the person so affected. [47] The IT Amendment Act, 2008 inserted a provision which provides that if any person or intermediary has obtained access to personal information of an individual while providing service, and thereafter if the former discloses the information of the latter, contrary to the contractual term, with an intention to cause wrongful loss or gain, the person so unauthorizedly disclosing the data will be liable for imprisonment for maximum three years or fine up to 5 lakhs rupees or both.[48]

G. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 provide for formulating policy with regard to the privacy and disclosure of personal and sensitive data. According to the rules the body corporate which is collecting, receiving, possessing, storing, or handling data of the individuals, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information thereby to ensure that the same are accessible by the data providers. Such policy shall be made available on the website of body corporate or any person on its behalf.[49]

Rule 3 categorize certain data as Sensitive Personal Data which also includes physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information, etc. The rule obliges the body corporate to secure consent from the individuals providing the sensitive

[47]The Information Technology Act, The Gazette of India, s. 43A (2000).

[48] *Id*. At s. 72A (2000).

[49]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, Ministry of Communications and Information Technology, r.4 (2011).

personal data with respect to its usage, before collection of such information. Even the disclosure of sensitive personal data or information by body corporate to any third party is not allowed without prior permission of the data, unless such disclosure has been agreed to in the contract. [50]

H. The National Medical Commission Act, 2019 and The Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002 ("MCI Code")

Health information needs to be kept confidential under the Medical Codes. The idea of confidentiality of the health information is ayurvedic in nature. Hippocratic Oath too binds the doctors or health care service providers to keep the secrets of their patients. In India, Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002 provide that the physicians shall never reveal any confidential or domestic matter of his patients that entrusted to him by the latter during medical treatment or consultation unless required by the laws of the State. The code also requires efforts to computerize medical records for easy retrieval of them. Alongside, the National Medical Commission Act, 2019 provides that the Central Government shall constitute certain Autonomous Boards, under the overall supervision of the National Medical Commission, to perform the functions assigned to such Boards. One of such Autonomous Boards is the Ethics and Medical Registration Board which has main function to regulate professional conduct and promote medical ethics.

I. Electronic Health Records Standards, 2016 (EHR Standards)

Electronic Health Records Standards, 2016 prescribes privacy standards relating to the collected health records from patient. This includes records from medical organizations also from medical equipment. The government has laid down standards for data protection realizing the need for it and made provisions relating to data capture, storage, recovery, exchange and analytics, and also includes, medical codes. The standards emphasize on the data ownership. It says that the patients are the real owners and deciders of their health data. Patients can access their health data. If the medical organizations having control over health data want to share that information with third party, the explicit consent of the patient is required. Healthcare service providers are made responsible for providing security to the health data. Encryption technology needs to be installed in order to secure the electronic information. Any

[50] *Id.*at r. 3.

information which discloses the identity of the patient should be strictly protected. Health data should be removed after achieving the intended purposes. Use of artificial intelligence in health care services by doctors, hospitals, pharmaceuticals, etc. is also subject to the above mentioned statutes.

V. Critical Evaluation

A major concern in privacy analysis is whether the individual has approved specific uses of his or her personal data.[51]The implementation of AI technologies in the healthcare systems has become evidently complex as this mechanism requires a huge amount of data for its functioning and those data is being stockpiled and handled by the data controller. Further present the treatment of the patient is highly dependent on the proficiency of persons from number of organizations and groups, which denotes the sharing of these health data with all of them as also discussed above. There is a high probability and prevalence of unqualified misuse of these personal health data by the data controller, by the government and other stakeholders. Now the fundamental questions are that: Whether the existing legal framework in India is sufficient enough to permit the health data of the individuals to flow suitably in this new edifice of healthcare system? Is the degree of privacy protection in healthcare ecosystem in India is adequate to accommodate the faith of the patient to share his or her personal sensitive data?

Analyzing the ongoing complex healthcare ecosystem based on complied dataset of the individuals and the existing legal framework, it is evidently clear that there exists a lot of loopholes and dangers that pose threat to the individual privacy. Following components are missing in existing framework:

A. Government's Access to Health Data, Due Process and the Actuarial Justice System

Health data is personal and sensitive information. For lawful purposes, both public and private bodies may have an access to an individual's health information. Access to health data stored on the intermediaries' databases is also allowed to the lawful enforcement agencies for the prevention of crime; for the investigation of crime; for the identification of suspect, etc;

[51] Legal frameworks for eHealth, WHO Global Observatory for eHealth series - Volume 5, (May 11, 2021, 08:40 AM) https://apps.who.int/iris/bitstream/handle/10665/44807/9789241503143_eng.pdf?sequence=1&isAllowed=y .

for the medical emergency; and for executing health schemes and policies. Since every access is an interference with an individual's right to privacy, which is fundamental right under Article 21 of the Indian Constitution, it is essential that the access must be in accordance with the due process of law. Due process further demands the fulfilment of the principles of proportionality, transparency, accountability and good governance.[52] Principles of checks and balances require that independent oversight mechanism to monitor the government's access and processing of health data should be established.[53]

The rise of Preventive State tends to use Big Health Data Analytics for fulfilling the purposes of the actuarial justice system. It seriously affects the vulnerable identities. People get discriminated on the basis of race, caste, ethnicity, religion, colour, body, and so on and so forth. Preventive justice cannot undermine the spirit of criminal justice jurisprudence.

B. Right to have Informed Consent and Right to Access to Health Information

As in machine learning, where the medical information is used to train and develop algorithms, a question of informed consent raises. Many patients though do not oppose using their data to advance health care delivery and research, but they should be asked to for prior permission before using those. Furthermore, even if consent is taken from the patients for using their sensitive health data for their treatment, it raises serious challenges in the prospective use. It would not amount to a truly informed consent, if patients are requested to sign up an extensive terms and conditions form before each episode of treatment or to approve the future uses of their personal medical information of which they are not at all "informed."

If the patients are not capable to participate in the decision-making processes relating to his or her health information, the hospital or doctors could misuse the consent given by the patients. This issue was particularly recognized by the Supreme Court in Samira Kohli v. Dr. Prabha Manchanda, where it observed that a huge number of patients in India fall under the BPL category who do have access to prepared medical care, and

[52] K.S. Puttaswamy v. Union of India, 10 SCC 1, 188 (SC:2017).

[53] Institute of Medicine (US) Committee on Assuring the Health of the Public in the 21st Century, The Future of the Public's Health in the 21st Century, NCBI (May 10, 2021, 10:32 AM), https://www.ncbi.nlm.nih.gov/books/NBK221231/.

thus having no choice except to avail the accessible treatment without query.

In India, the large population is uninformed about the processing of their health information. Poverty, illiteracy, poor accessibilities to the health services, lack of infrastructure, etc. created the digital divide among the citizens in the new media world. Unawareness and uninformed consent does not let the individual to act autonomously. It also affects the psychological well-being of the individual. The overall effect of the unawareness and uninformed consent would defect the public functions of the health services in India. According to the PwC Health Research Institute Analysis (2018), only 55% of healthcare providers said they implemented security controls, while 37% didn't even think to perform a risk assessment on their medical devices.[54]

Right to access the health data empowers the data subject to participate in the respective decision-making processes. It allows the individual to correct and update his or her health information. Automatic processing of incomplete or wrong information may subject the concerned individual to mental agony or harassment caused by the police powers of the State. It is arbitrary exercise of powers. For example, quarantine powers, which are police powers of the State during the pandemic period, can be abused due to the incorrect information. Right to update the health information prevents such kind of injustices.

C. Reasonable Expectation of Privacy

An individual has reasonable expectation of privacy in his or her health information given either to public or private entity. The individual does not want that his or her health information should be subjected to public humiliation or harassment. If the health data controllers fail to protect the confidentiality of an individual's information, it causes his or her both material and non-material loss, which include emotional and psychological distress.

[54] PwC Health Research Institute, Global Top Health Industry Issues: Defining the Healthcare Of The Future, PWC, (May 13, 2021, 10:32 AM), https://www.pwc.com/gx/en/healthcare/pdf/global-top-health-industry-issues-2018-pwc.pdf.

D. Conflict between the Laws

There are certain laws like the Aadhar Act, 2017 which provides for the mandatory biometric data of the individuals to create the unique identification number of each individual. This very Aadhar card is the being made the license to various basic facilities to citizens, as the Public Distribution system, opening of bank account, etc. India's "Aadhaar" system with a centralized database, aims to deliver services by reducing frauds and increasing competences.[55] In one hand, the legislature through such law is authorizing the government to ask for the biometric data of the individual, where individual has no other option than to surrender to such rules to access the basic facilities. Whereas, on the other hand it has made laws and rules (IT Rules, EHR Standards) which provides that the individual can only be the owner of his data and without his consent no personal data can be shared with third party. So, the former and the latter rules create a deadlock. The beneficiaries of the latter rules are made obligatory by the former rule to provide their personal data. Moreover, the Aadhaar system also signifies extensive digital biometric identity structure organized during its initial years without direct legislative privacy, or ethical limits.[56]

VI. Conclusion and Way Forward

The issue that relates AI and data protection, particularly in healthcare sector is a key problem that needs to be addressed. It is expected that within 5 years AI is to overtake the human intelligence.[57] So there is an urgent need to enact laws to regulate its functioning. Express statutes are not exhaustive in nature and though seek to provide for data protection, its implementation have to be ensured. In order to cope up with the problems created due to AI, the jurisprudential concept of right to privacy would always be helpful. Issues

---

[55] Pam Dixon, A Failure to "Do No Harm" -- India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., (May. 12, 2021, 04:54 PM) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5741784/.

[56] *Ib.*

[57] Elon Musk Thinks that Artificial Intelligence Will Be 'Vastly Smarter' Than Humans in 5 Years, News 18, (May. 20, 2021, 04:54 PM) https://www.news18.com/news/buzz/elon-musk-thinks-that-artificial-intelligence-will-be-vastly-smarter-than-humans-in-5-years-741359.html#:~:text=Tesla%20and%20SpaceX%20CEO%20Elon,would%20overtake%20us%20by%202025.&text=He%20even%20described%20AI%20as,very%20careful%20about%20artificial%20intelligence.

which are not yet explored can be answered with the functions of right to privacy. Right to refuse medical treatment, right to be notified about the privacy violations, right to compensation, etc. are part of right to privacy.

Right to privacy is enforceable against the private actors as well. As discussed above, healthcare service providers using artificial intelligence has the potential to affect the individuals' right to privacy. Also, the passage of the PDP Bill, 2018 can be considered as a desirable step in this regard which would exhaustively deals with data protection and categorize health data as sensitive personal data and processing of it is subject only to certain grounds such as, explicit consent, or in compliance with law or order of the court, or for certain function of the state, or for any prompt action. However, it is suggested that the DPA set by the PDP Bill must be an independent authority to effectively ensure the goal of data protection. These provisions are certainly for the improvement of delivery of healthcare, though its efficacy is yet to be perceived.

a. **Proportionate use of Preventive System by State, Due Process and Democratization of Health Data**

In case where an individual's health information is identifiable and subject to the police powers of the State, both ex-ante and ex-post judicial review should be applied, which is a part of the quality rule of law. It limits the clandestine powers of the executive to access the health data by the use of the means of artificial intelligence.

Preventive justice as discussed above cannot be applied in isolation. It is also bound to follow the just, fair, and reasonable due process of law as is read into Article 21 of our constitution. Reviewing bodies that monitor preventive powers of the State should be independent in nature, and the victims of the unconstitutional uses of the health data must be notified about their right to remedy and compensation by the oversight body.

The current unprecedented capabilities of the artificial intelligence in health care services, which enable the government and non-government bodies to conduct mass surveillance over the health status of the whole population, are needed to be regulated by the constitutional democracy. Democratization of the Big Health Data may serve the purpose which entails participation of the people. It ensures a world where patients will be armed with data, technological skills, and access to expertise knowledge. Therefore, they can take charge of their own well-being and be able to manage their own health. Democratization can also be assured by the enablement of the AI-based technologies like the

wearable devices (fitness bands), glucometer (accu-check). In this respect it should also be remembered that, the laws and policies in relation to the Big Health Data cannot be passed hurriedly and without debates and discussions. Inclusive democracy decides the requirement, extent and scope of the collection of health data for constitutional purposes. Also, bypassing the standards of inclusiveness is an excessive delegation of the legislative powers of the Parliament.

Health data should be protected against all sorts of unauthorized accesses. For the purposes of providing security, it is necessary to conduct risk or impact assessments of the collection and processing of the health data. Adequate safeguards, including administrative, physical, and technical, should protect the confidentiality and integrity of the health information system. Anonymity of the health data prevents the abuse of the vulnerable identities. It removes the personally identifiable information from the health data, and makes the information anonymous. Further, collection of identifiable information should be minimum and compatible with the purpose. Even the de-identified information should be regulated. For the artificial intelligence technology is smart enough to make it personally identifiable. Once the purpose of collection and processing is achieved, the retention of the health data becomes unjustified and unreasonable. The data controllers cannot retain it without explicit consent of the data subject. The data subjects have right to erase their health data. Recently, the Delhi High Court recognized the right to be forgotten in an interim order and directed Google and Indian Kanoon to take down a judgment relating to an American citizen of Indian origin.[58] So this right to be forgotten/right to erasure can also be exercised for the protection of the personal health data carrying varying identifying characteristics of the individual.

Moreover, the recent Consumer Protection Act has also tried its best to secure the interest of the consumers i.e., the individuals relating to their personal data, but how far it will be implemented is a big question. As many of the consumer are unaware as to how and where their data are used by the data fiduciaries. So firstly, the individual consumers or the patients should be made mindful about

[58] Apoorva Mandhani, Do you have a 'right to be forgotten'? Here's what it means and how Indian courts view it, The Print, (May 14, 2021, 09:50 AM) https://theprint.in/judiciary/do-you-have-a-right-to-be-forgotten-heres-what-it-means-and-how-indian-courts-view-it/666226/.

their rights and possibility of data breach by the data fiduciaries, so that they remain alert and active enough to enforce their rights.

It is high time that the judicial system needs to adopt a standard for AI and develop the jurisprudence in this regard, where the manufacturers and developers agree to abide by general ethical guidelines, such as by way of adopting a mechanical standard enshrined in any international instrument. And this standard may be applied when there are chances of foreseeability that the data and algorithms can cause substantial injury and damage to the interest of the consumer or the customer on whom is it applied. Weak regulation and enforcement structure will certainly create low right environment. There is also a need to bring forth transparency or accountability in the operation of AI.

Without access to justice, right to remedy and compensation is ineffectual. Therefore, it is necessary that the victim of the unlawful processing of the health data should have access to an independent tribunal or court. The victim should be remedied for all damages This tribunal or court must have sufficient powers to redress the grievances.