NLUJ Law Review

Subhradipta Sarkar, *Impact of Artificial Intelligence in Healthcare in India: Exploring the Issue of Legal Liability*, 8(1) NLUJ L. REV. 90 (2021).

IMPACT OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE IN INDIA: EXPLORING THE ISSUE OF LEGAL LIABILITY

*Subhradipta Sarkar**

ABSTRACT

Healthcare has been one of India's most rapidly expanding industries. Yet the Indian healthcare system continues to be plagued by several problems. On this front, artificial intelligence (AI) provides a promising response to various diagnoses and prognoses. However, it equally presents challenges to patient safety, ascertaining legal liability and data security. Considering the complex technology and large number of actors involved in the AI processes, discovering the fault lines is challenging. Apprehensions are ripe that AI would foster the growth of 'black-box medicines' leading to opaque computational models of decision-making; and hence, creating ambiguity in negligence cases. Efforts are on in building 'explainable AI'. Furthermore, concern remains regarding the 'right to privacy' with regard to the protection of the large amount of healthcare data of patients, especially after the Sprinklr controversy that arose in the context of the Covid-19 patients in Kerala. Notwithstanding the fact that the new Personal Data Protection Bill of 2019 has classified "health data" as

* The author is an Associate Professor of Law at Jamia Millia Islamia, New Delhi and may be contacted at **ssarkar@jmi.ac.in**. The author would like to appreciate and acknowledge the contribution of Mr. Akshay Luhadia, penultimate year student of the West Bengal National University of Juridical Sciences as a Research Assistant for this paper.

"sensitive personal data" and has provided protection, it has also created exceptions for accessing the same. With over 70 per cent of the healthcare in the private hands, acquiring these data sets in developing algorithms and their subsequent sharing raise serious privacy concerns.

TABLE OF CONTENTS

I. INTRODUCTION

Healthcare is one of the most vibrant and growing fields in India. In 2018, the NITI Aayog projected the sector to grow to USD 280 billion by 2020, at an annual growth crossing 16 percent.[342] Nevertheless, it didn't miss to mention the ordeals ranging from acute shortage of qualified professionals to unaffordability, which continues to plague the Indian healthcare system. It is anticipated that Artificial Intelligence [*hereinafter* "**AI**"] and related technologies could be utilized to negate those problems to a large extent.[343]

The potential for AI in healthcare is enormous and it is getting increasingly better at doing human tasks, with greater efficiency and at a lower cost.[344] Specific algorithms have already begun to outdo radiologists in detecting the whereabouts of malignant tumours, and manoeuvre ways for inventing alternatives to expensive clinical trials.[345] AI helps in evaluating information from a particular patient by comparing it with a large dataset from different patients. Correlations are detected and diagnoses are suggested by the self-learning programmes.[346] Yet there are numerous

---

[342] NITI AAYOG, NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE 13 (2018), *available at* https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf (last visited May 31, 2021) ("**NITI AAYOG**").
[343] *See generally id* at 24 – 26.
[344] *See* Roland Wiring, *Digitisation in Healthcare: From Utopia to Reality – Artificial Intelligence, Its Legal Risks and Side Effects,* CMS (September 2018), *available at* https://cms.law/en/che/publication/digitisation-in-healthcare-from-utopia-to-reality-artificial-intelligence-its-legal-risks-and-side-effects.
[345] *See* Thomas Davenport and Ravi Kalakota, *The Potential of Artificial Intelligence in Healthcare*, 6 FUTURE HEALTHCARE J 90, 94 (2019).
[346] *See id.*

challenges that lie in front of us before AI-enabled robots replace human doctors. Patients' safety is paramount in medical treatment, and it aims to reduce harm or prevent patients' exposure to risks during provision of health care.[347] Today we are confronted with various issues involving AI which have the potential to threaten patient safety. Till date, AI is not regulated by any specific legislation, so if any diagnosis or surgery goes wrong and results in harm to the patient, there is an uncertainty with regard to civil liability. Who do we hold liable – the AI-provider, the doctor or both?

While the technology promises to deliver quicker and more accurate results, apprehensions are ripe if AI would foster the growth of 'black-box medicines' leading to opaque computational models of decision-making. Their predictions are based on algorithms and not on medical understanding, making their decisions opaque; and hence, creating ambiguity in negligence claims. Additionally, if we seek to regulate AI-based products, there is a need to examine if they qualify as "product liability" under the Consumer Protection Act, 2019.[348] Furthermore, data is at the heart of AI activities. As a result, safeguarding patients' sensitive health data remains a challenge, particularly after the Supreme Court of India [*hereinafter* "**the Supreme Court**"] declared the "right to privacy" a Fundamental Right.[349] The existing legal regime on data protection is regrettably

[347] World Health Organisation, *Patient Safety* (Sep. 13, 2019), *available at* https://www.who.int/news-room/fact-sheets/detail/patient-safety.
[348] Consumer Protection Act, 2019, Act No. 35, Acts of Parliament, 2019 (India).
[349] Justice K.S. Puttawswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

inadequate and the proposed Personal Data Protection Bill, 2019, also poses certain apprehensions. Over 70 per cent of the healthcare expenditure is done by private entities,[350] resulting in large scale presence of the private players in the healthcare sector. As patients visit those private places for treatment, the private entities will resultantly also acquire the patients' data to develop algorithms and become the repository of that data. Consequently, sharing of the data for its usage/storage raises serious privacy concerns.

In this paper, Section II deals with certain basic concepts relating to AI and its implication on healthcare. Section III highlights some major challenges facing Indian healthcare systems and AI initiatives that may go a long way in dealing with these challenges. Section IV elaborates the legal debate in cases of misdiagnosis when patients are treated with the help of AI devices; it delves into the question of negligence, fault-based liability and even the feasibility of drawing strict product liability. As data remains the primary component of AI, protection of patient's data remains a major concern. Therefore, Section V deals with the concerns regarding protection of data. It discusses the legal regime on data protection in India and abroad and draws instances to substantiate the arguments. In Section VI, the author concludes that there are still unsettled issues and thus, endeavours to provide some suggestions towards possible legal solutions.

[350] NITI AAYOG, *supra* note 342, at 26.

II. BASIC CONCEPTS RELATING TO AI AND ITS IMPLICATIONS ON HEALTHCARE

AI entails a variety of algorithms which provide computers the capability to complete tasks which would otherwise require human effort and problem-solving skills. Although AI remains one of the latest trends in the field of engineering, it has been in discussion since 1950s.[351] It was declared as "*the science and engineering of making intelligent machines*" by John McCarthy, one of the founding fathers of AI.[352] To be considered intelligent, according to another AI great, Alan Turing, a computer must be proficient in executing nearly equivalent tasks as a human.[353] AI has been created since then to emulate human reasoning, decision making, knowledge representation, complicated task processing, and exchange of information.[354] AI has also been hailed as the dominant actor for the impending fourth industrial revolution.[355] Stuart J. Russell and Peter Norvig defined AI as a collection of systems with the ability to think, act and rationalise like humans. It's a set of algorithms that allow select machines to operate more efficiently and accurately, emulating human comprehension abilities.[356]

---

351 *See* Sandeep Reddy, John Fox and Maulik P Purohit, *Artificial Intelligence-enabled Healthcare Delivery*, 122(1) J. ROYAL SOC'Y OF MEDICINE 22 (2018) ("**Reddy**").
352 *See id.*
353 *See id.*
354 *See id.* at 2.
355 *See id.*
356 *See* Paulius Cerka, Jurigta Grigiene and Gintare Sirbikyte, *Liability for Damages Caused by Artificial Intelligence*, 30 COMPUTER L & SECURITY REV. 1, 3 (2015) ("**Cerka et al**").

Before we delve into the nuances of the problem at hand, there is a need to highlight a few basic concepts related to AI. Machine learning [*hereinafter* "**ML**"] process is an integral part of AI. Artur Samuel coined the term in 1959 to mean "*the ability to learn without being explicitly programmed*".[357] ML represents that class of machines with the unique capability to shadow human behaviour using aggressive data mining methods such as sensors, metadata input systems and algorithmic protocols, in addition to trailing humans. The ability also accords machines to improvise their functionality sans any overt act by humans.[358]

Deep learning [*hereinafter* "**DL**"] is another important subset of AI. DL is a technique for implementing ML. It offers a technology or network proficiency in data learning that isn't supervised. It acts as a self-sufficient component of AI which works like human brains interconnecting neurons.[359] In fact, Artificial Neural Networks [*hereinafter* "**ANNs**"] are essentially modelled off the biological structure of a brain. The neurons in ANN have distinct layers and are connected with other neurons. A layer is the highest-level building block in DL, which usually obtains weighted input, converts it with a batch of generally non-linear functions and then

---

[357] NITI AAYOG, *supra* note 342, at 14.
[358] *See* Adam Tabriz, *Medico-legal Perils of Artificial Intelligence and Deep Learning*, DATA DRIVEN INVESTOR (Oct. 24, 2019), https://www.datadriveninvestor.com/2019/10/24/medico-legal-perils-of-artificial-intelligence-and-deep-learning/.
[359] *See* NITI AAYOG, *supra* note 342, at 14.

transmits these values as output to the subsequent layer.[360] This very layering has provided deep learning with its name – the more the depth, the greater the learning, which is created by multiple layers.[361] ANN is a complex adaptive system, that means it is capable of altering its inner construction mostly based on the data flowing by it.[362]

III. INDIA'S HEALTHCARE PROBLEMS AND AI APPLICATIONS

NITI Aayog's National Strategy for AI has identified some major deficiencies in our health care sector, *e.g.*, shortfall of qualified healthcare professionals and services compared to World Health Organisation guidelines, wide disparity of healthcare services between urban and rural India, high out-of-pocket expenses making healthcare unaffordable for majority of the population, and reactive approach to essential healthcare.[363]

In such a scenario, it is hoped that greater use of AI would be able to address many of the above-mentioned problems. *E.g.,* in India, while each year new cancer patients grow by more than a million, we have only 2,000 pathologists experienced in oncology.[364] Therefore, large-scale cancer screening possesses a humongous opportunity for AI-induced interventions. ML solutions can assist a general pathologist in performing

---

[360] *See* Academy of Medical Royal Colleges, *Artificial Intelligence in Healthcare* 8 (Jan. 2019), https://www.aomrc.org.uk/wp-content/uploads/2019/01/Artificial_intelligence_in_healthcare_0119.pdf (last visited May 31, 2021).
[361] *See* NITI AAYOG, *supra* note 342, at 13.
[362] *See* Cerka *et al.*, *supra* note 356, at 5.
[363] *See generally* NITI AAYOG, *supra* note 342, at 24 – 26.
[364] *See id.* at 28.

cancer diagnosis and bridge the aforementioned gap.[365] Further, the use of AI is believed to replace current techniques employed by clinicians with greater accuracy, reliability and efficiency.[366] The American Cancer Society has noted that a high number of mammograms produce false positives. Switching to AI allows a 99 percent accuracy along with the process being 30 percent times faster.[367]

Many technology companies which have developed AI applications are significantly revolutionizing the health sector by supporting both patients and healthcare professionals. Several initiatives, both private and governmental, have started in India. NITI Aayog has initiated a partnership with Microsoft in addition to Forus Health to work on eye-check-ups.[368] Max Healthcare claimed that the usage of AI technology drove the cost of critical care down by almost 30 per cent by the efficient use of the ICU ward.[369]

---

365 *See id.* at 29.

366 *See generally* Fei Jiang *et al.*, *Artificial Intelligence in Healthcare; Past, Present and Future*, 2(4) STROKE AND VASCULAR NEUROLOGY 230, (2017).

367 Tejal A. Patel *et al.*, *Correlating mammographic and pathologic findings in clinical decision support using natural language processing and data mining methods,* 123 (1) CANCER 114, 117 (2016); Sarah Griffiths, *This AI Software Can Tell if You're at Risk from Cancer Before Symptoms Appear*, WIRED (Aug. 26, 2016), http://www.wired.co.uk/article/cancer-risk-ai-mammograms (last visited May 31, 2021).

368 *See* NITI AAYOG, *supra* note 342, at 29.

369 *Indian Healthcare is All Set to be Transformed by AI*, MEDICAL BUYER, (Mar. 5, 2019), https://www.medicalbuyer.co.in/indian-healthcare-is-all-set-to-be-transformed-by-ai/.

IV. THE LIABILITY DILEMMA

Nearly all AI solutions currently being developed are not strictly intended to be fully autonomous. The human hand, either directly or through the ability to override the machine, determines, directs, and eventually controls the programming process.[370] Despite all technological developments, AI clinicians comparable to human medical experts appear to be still a distant dream of the future. Nevertheless, the possibility of extensive use of AI tools by the clinicians is real and it presents a daunting task of ascertaining the liability in cases of misdiagnosis or mistreatment.[371]

According to Salmond, the bond of necessity that remains between the wrongdoer and the redress for the wrongdoing is known as liability. It implies the state of a person who has violated the right or acted in contrary to the duty.[372] In other words, the person who is at "fault" is obligated under the tort law to pay damages.[373] Therefore, when a clinician wrongly treats a patient with the approval of the AI diagnostic tool, who becomes liable? The challenge is to ascertain as to where does the fault lies – the clinician or software developer or the medical establishment where the clinician is employed and the AI tool is maintained?

---

[370] *See* Vladeck C. David, *Machines without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 120 (2014).
[371] Anastasia Greenberg, *McGill Intelligence in Health Care: Are the Legal Algorithms Ready for the Future*, MCGILL J. L. AND HEALTH (2017), ("**Greenberg**").
[372] *See* V. D. MAHAJAN, JURISPRUDENCE AND LEGAL THEORY 365 (5th ed., 1987).
[373] Emiliano Marchisio, *In support of "no-fault" civil liability rules for artificial intelligence*, 1 SN SOCIAL SCIENCE 54, 56 (2021) ("**Marchisio**").

A. MEDICAL NEGLIGENCE AND THE DOCTRINE OF *RES IPSA LOQUITUR*

In case of an injury resulting from medical misdiagnosis or mistreatment, liability is derived from the tort of negligence committed by medical professionals. A three-stage procedure must be conformed to assess negligence: (i) the defendant had a "duty of care" towards the plaintiff; (ii) the defendant violated that duty; and (iii) consequently, the plaintiff suffered legally recognised harm. If the plaintiff's case is successful, the defendant will be held liable for damages.[374] The Supreme Court in *Jacob Mathew v. State of Punjab* [375] [*hereinafter* "***Jacob Mathew***"] sought to distinguish between occupational negligence and professional negligence. Adopting a liberal approach, the Supreme Court concluded that a careless attitude, a mistake of judgement or an accident, cannot be said to be a case of medical negligence. Provided that a clinician observes and adheres to the accepted method of the medical profession at the time, he cannot be held liable only since a better therapy exists or a more effective clinician may not have followed the same method.[376] Inability in taking special or unusual steps that might have avoided the actual occurrence cannot be used to judge the suspected negligence.[377]

A clinician can be held responsible for negligence when either he was found unable to perform certain skills which he professed to have or

---

[374] *See* W.V.H. ROGERS, WINFIELD AND JOLOWICZ ON TORT 150 (18th ed., 2010).
[375] Jacob Mathew v. State of Punjab, A.I.R. 2005 S.C. 3180.
[376] *See id.* at ¶ 49(2).
[377] *See id.*

he did not proceed with the due diligence required of a prudent man. It's a utopian idea for every professional to command the highest degree of knowledge or skill in the area of his practice. Hence, the standard for judging negligence of an individual, might be that of a professional individual in that field performing standard tasks.[378] The method depends on finding faults caused by the doctor, hospital, and others to ascertain medical negligence. The plaintiff must prove on the basis of probability that the hospital or doctor (the defendant) was negligent.[379]

In cases of negligence, *prima facie*, it is for the plaintiff to satisfy the courts that the harm has happened due to the defendant's negligence. However, in many cases it has been difficult for the plaintiff to adduce enough evidence about negligence to sustain his/her claims.[380] To obviate such a hardship, a presumption is required to be made about the factum of negligence in the happening of an unfortunate accident in view of the evolution of the doctrine of "*res ipsa loquitur*". The doctrine refers to an implication of negligence being drawn against the defendant as a result of the occurrence of certain events.[381]

In *Lloyde v. West Midlands Gas Board*,[382] Megaw L. J. explains that as the plaintiff *prima facie* establishes negligence as per this doctrine when, (a) he cannot exactly explain the relevant act or omission that gradually led to

---

[378] *See id.*
[379] *See* Daniele Bryden and Ian Storey, *Duty of care and medical negligence Continuing Education in Anaesthesi*a, 11(4) CRITICAL CARE & PAIN J. 124, 124 (2011).
[380] *See* JOHN MURPHY, STREET ON TORTS 249 (2007).
[381] Manubhai Punamchand Upadhya v. Indian Railways, 1997 A.C.J. 1270, ¶14.
[382] Lloyde v. West Midlands Gas Board, (1971) 2 All E.R. 1240.

the accident; and (b) the potent cause of the accident was any act or omission of the defendant or another person for whom the defendant is responsible, according to the evidence as it stands at the relevant time.

Indian courts have employed this doctrine in medical negligence cases. In the famous case of *Mrs. Aparna Dutta v. Apollo Hospital Enterprises Ltd.*,[383] the plaintiff was subjected to an operation (in the defendant's hospital) for removal of her uterus, as she was diagnosed to have cyst in one of her ovaries. After the operation, she continued to suffer from severe pain, she had to, unfortunately, undergo another surgery to get the abdominal pack removed which was left by the first surgeon. In an action claim of negligence, the court determined that leaving a foreign matter in the body during the procedure was a case of *res ipsa loquitur* as no other explanation for the presence of the abdominal pack is plausible.[384] The plaintiff was paid compensation.

We are still in the nascent stages of using AI and the medical community is yet to lay down any acceptable protocols involving AI tools. Unless such protocols are laid down, given the *Jacob Mathew* judgement, it would be extremely difficult for the judges to decide if the clinician in question is negligent. Under the existing medico-legal liability regime, often the traces of liabilities are ambiguous when medical errors occur; and it would become even more debatable when more and more autonomously designed AI 'agents' start delivering healthcare services.[385] In such cases,

---

[383] Mrs. Aparna Dutta v Apollo Hospital Enterprises Ltd, A.I.R. 2000 Mad. 340.
[384] *See id.* ¶ 23.
[385] *See* Reddy, *supra* note 351, at 4.

applying the doctrine of "*res ipsa loquitur*", a presumption of liability on the part of the clinicians and/or hospitals may be derived. They may be held liable for failing to take the necessary precautions before deploying AI tools or procedures to treat patients.

B. PRODUCT LIABILITY AND ITS LIMITATION

Some experts feel that the claims and success of AI are overblown. In recent times, the outcome of the accidents involving Tesla's semi-autonomous cars in the United States is relevant to that point. It has important ramification on the question of liability involving AI tools in healthcare. Because Tesla had been aggressively advertising about their cars' full self-driving capabilities, drivers over-relied on the ability of those cars and did not take active participation in the driving or they remained distracted, *e.g.*, playing cell phone games in one case. In the exemplified case in 2018, the driver died when his car, in auto-pilot mode, hit a concrete barrier on a Silicon Valley Freeway.[386] Eventually, the National Transportation Safety Board [*hereinafter* "**NTSB**"] found that the cars in question had limitations on self-driving mode with respect to driver distraction, level of driver engagement and collision avoidance system. However, the regulators failed to take note of the limitations of safety measures built in those cars. The NTSB found the victim-driver negligent in the act and held Tesla only partially liable for the accidents and

[386] *See* Rebecca Heilweil, *Tesla Needs to Fix Its Deadly Autopilot Problem,* VOX (Feb. 26, 2020), https://www.vox.com/recode/2020/2/26/21154502/tesla-autopilot-fatal-crashes.

recommended for more oversight of such cars by appropriate authorities.[387] In the absence of fully AI-driven clinicians or programmes, it is the humans who either manage them or eventually act on the diagnoses. Therefore, in a comparable situation we can say that the operator/clinician will most probably be held liable for any resultant harm.

There are certain inherent problems with AI usage in healthcare, especially in the realm of legal liability. ML has the ability to intake intricate data consisting of millions of gigabytes. Algorithms are trained to generate classifications or predictions using statistical approaches and improvise the machines.[388] The higher the complexity of the data which the machine is trained on, the better and more accurate results it can produce. In fact, there has been a rapid increase in the collection of health data today than ever before. Gradual transition of this data in electronic form, known as 'Electronic Health Records' [*hereinafter* "**EHRs**"], has served a variety of reasons: from enhancing efficiency in patient care to maintaining records for settling insurance claims and preventing malpractices.[389] Nonetheless, there's a danger of 'overfitting'. It happens when algorithms learn modelling datasets to an extent that it can't efficiently simplify on a new dataset – one

---

[387] *See Collision Between a Sport Utlity Vehicle Operating with Partial Driving Automation and a Crash Attenuator Mountain View, California*, National TRANSPORT SAFETY BOARD (Mar. 23, 2018), https://www.ntsb.gov/news/events/Documents/2020-HWY18FH011-BMG-abstract.pdf.

[388] *See* Reddy, *supra* note 351, at 2.

[389] *See* W. Nicholson Price II, *Black-Box Medicine*, 28(2) HARVARD J. L. & TECH. 419, 430 – 31 (2015) ("**W. Nicholson Price II**").

used in making decisions about new patients.[390] For example, any ML trained on data that over-represents white patients, may give the wrong diagnosis regarding coloured patients.[391] Hence, diligent ML researchers consistently find new types of data problems or sets for their machines to analyse the reliability of the machine and just how generalizable their machines are. Error, although, as in humans, is inevitable.[392] Such may lead to a case of misdiagnosis.

i. Inexplicability Surrounding Black-box Medicines

The introduction of AI will lead to the growth of "black-box medicine" which are principally based on opaque computational models. In AI systems, input data and output decisions are known, but exact steps taken by the computer and software to reach the decision cannot always be fully retracted. This process is known as "black box".[393] As the name suggests, the machine is learning about the data patterns rather autonomously. Even the developers of the AI systems are ignorant about the process of reaching the conclusions by the systems.[394] One of the defining characteristics of black box medicine is that it cannot explain its

---

[390] *See* Jason Brownlee, *Overfitting and Underfitting with Machine Learning Algorithms*, MACHINE LEARNING MASTERY, (Mar. 21, 2016), https://machinelearningmastery.com/overfitting-and-underfitting-with-machine-learning-algorithms/.

[391] *See* Olivia Goldhill, *When AI in healthcare goes wrong, who is responsible?*, QUARTZ (Sep. 20, 2020), https://qz.com/1905712/when-ai-in-healthcare-goes-wrong-who-is-responsible-2/ ("**Goldhill**").

[392] *See* Greenberg, *supra* note 371, at 7.

[393] *See generally* W. Nicholson Price II, *supra* note 389, at 2.

[394] *See* Liz Szabo, *A Reality Check on Artificial Intelligence: Are Health Care Claim Overblown*, KHN (Dec. 30, 2019), https://khn.org/news/a-reality-check-on-artificial-intelligence-are-health-care-claims-overblown/.

findings; in that way it is non-transparent. It does not base its findings on sound medical knowledge, rather its purely a prediction based on the working of an algorithm.[395] To neutralize this problem, researchers are trying to develop "explainable AI" which are ML algorithms that are inherently explainable. Thus, "explainability" can explain how decisions are drawn, allowing for better future decision-making as well as inspection and traceability of AI behaviour. Humans will be able to get into AI decision loops and stop or monitor their tasks as required thanks to traceability. An AI system is supposed to not only complete a task or make decisions, but also provide a model that can include a clear report on why it reached those conclusions.[396]

Gabriela Bar, an expert in the law of new technologies, suggests AI systems should be explainable by design. She refers to European Commission's White Paper on Artificial Intelligence of 2020 which emphasises that future AI regulatory framework should include the types of legal obligations to be imposed on entities involved in all stages of AI operations from designers to end-users.[397] However, the transparency of AI operations and the explainability of its decisions can be a calibrated one as all entities involved do not require the same kind of information as to how

---

[395] *See* Susan Athey, *Beyond Prediction: Using Big Data for Policy Problems*, 355(6324) SCIENCE 483, 485 (2017).

[396] *See* Ron Schmelzer, *Understanding Explainable AI*, FORBES (Jul. 23, 2019), https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/?sh=264ef6f47c9e.

[397] *See* Gabriela Bar, *Explainability as a legal requirement for Artificial Intelligence*, MEDIUM (Nov. 27, 2020), https://medium.com/womeninai/explainability-as-a-legal-requirement-for-artificial-intelligence-systems-66da5a0aa693.

raw data and code translate into benefits or harms. Moreover, there could be intellectual property rights issues, so it is not always possible or necessary to explain the working of the AI completely. Nevertheless, there could be high-risk AI, *e.g.*, used in the healthcare sector, where such trade-offs should commensurate with risk assessment and the its impact on human life. In effect not only will public confidence in AI grow, but it will also assist us to ascertain appropriate liability in AI operations.[398]

On one hand, for competitive purposes, AI is deliberately hidden but on the other hand, some techniques are just above human understanding. ML technologies can be particularly opaque because they have the ability to adjust themselves through various small tweaks which change their parameters and the rules by which they operate. This causes issues when it comes to validating outputs for AI systems and detecting errors or biases in the data.[399] The House of Lords Select Committee on AI has already forewarned that the datasets available to machines do not properly represent the wider population and therefore could lead to prejudiced or unfair decisions that would further cause chaos.[400] IBM released an IBM Watson Oncology machine for diagnosing cancer. However, its use was halted in clinics because outside the US, doctors did not believe in its recommendations. They felt that the database used for

---

398 *See id.*

399 *See* Ran Svenning Berg, *Artificial Intelligence in Healthcare and Research,* NUFFIELD COUNCIL ON BIOETHICS, (May 15, 2018), https://www.nuffieldbioethics.org/publications/ai-in-healthcare-and-research.

400 *See id.*

cancer treatment was very American-oriented.[401] In such ambiguous cases, it's unclear where the fault ought to lie in case of any harm – whether with the ML company who collected biased data or the clinician who acted upon that recommendation.[402] Both the manufacturer and operator may be jointly held liable for any resultant damage suffered by the patient. The share of the burden may be determined by the judiciary on a case-to-case basis.

ii. Faculty Medical Devices and their Consequences

AI tools or programmes are designed or developed by another person and misdiagnosis or mistreatment may occur due to a faulty device. This could be beyond the know-how of the clinician, and hence, it brings us to the next probability, *i.e.,* the liability of the software developer or manufacturer for the flaws in manufacturing, design, or programming which might have caused the injury. This option would lie in the realm of product liability. Product liability also infers a certain onus on the manufacturer or vendor of the goods to compensate the injured due to defective merchandising that was available for sale.[403] The issues of product-liability have also led to the introduction of certain contract principles and tort principles as well. Here, the contract principle is based on 'warranty' whereas tort law product liability is propounded from

---

401 *See id.*

402 *See generally* Goldhill, *supra* note 391.

403 *See* Anindya Ghosh and Nabarun Chandra Ray, *India: Product Liability Law in India: An Evolution*, MONDAQ (Aug. 7, 2020), https://www.mondaq.com/india/dodd-frank-consumer-protection-act/974270/product-liability-law-in-india-an-evolution ("**Ghosh and Ray**").

'negligence' and 'strict liability'.[404] Through the passage of time, product liability jurisprudence has advanced along the lines of adjudging the manufacturer responsible for damages in cases of harm suffered by the eventual consumer as a result of a manufacturing error, despite the fact that there was no arrangement between the consumer and the manufacturer.[405]

Since AI is so recent with many unknown threats, it needs close monitoring. Yet the reality is juxtaposed. In a technologically advanced country like the United States, the majority of AI devices are exempted from US Food and Drug Administration [*hereinafter* "**FDA**"] approval.[406] Furthermore, the Nationwide Academy of Medicine asserts that there's been no serious analysis on whether 320,000 medical applications available today really enhance health.[407] Many of these application developers have never applied for FDA clearance, despite the fact that it is legally required. Furthermore, with subtle backing from the business lobby, legislative changes have been introduced to exempt countless medical software programmes from federal review, along with health apps, digital well-being information and instruments that assist doctors in making medical decisions.[408] For instance, in 2016, the Federal Food, Drug, and Cosmetic

---

[404] *See* VIVIENNE HARPWOOD, MODERN TORT LAW 335 – 36 (6th ed., 2005); *see also Products liability*, LEGAL INFORMATION INSTITUTE (CORNELL LAW SCHOOL), https://www.law.cornell.edu/wex/products_liability (last visited May 31, 2021).
[405] *See* Ghosh and Ray, *supra* note 403.
[406] *See Changes to Existing Medical Software Policies Resulting From Section 3060 of the 21st Century Cures Act*, FDA (Sep. 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act ("**FDA**").
[407] *See* Szabo, *supra* note 394.
[408] *See id.*

Act [*hereinafter* "**FD&C Act**"] was amended by the 21st Century Cures Act to removed certain software functions from the definition of 'device' under the FD&C Act.[409] Faulty or unregulated AI devices or programmes can wreak havoc. In recent years, the FDA has come under fire from various quarters, including the American Medical Association, for allowing hazardous medical devices to be sold, which the Consortium of Investigative Journalists has linked to nearly 80,000 fatalities and 1.7 million injuries over the last decade.[410]

Johnson & Johnson [*hereinafter* "**J&J**"] hip implant fiasco is well documented. Faulty hip implants manufactured by the company forced thousands of patients to undergo revision surgeries. Eventually the company was forced to recall the implants worldwide and pay millions of dollars in compensation.[411] Indian patients also suffered the brunt of the problem. The Government set up an expert committee at both the centre and state-levels. It was found that J&J suppressed the fact of the adverse effects of such faculty hip implant from the regulators. In India, based on the recommendation of the expert committees, the Central Drugs Standard Control Organisation [*hereinafter* "**CDSCO**"], equivalent to the US FDA,

---

409 FDA, *supra* note 406.
410 *See* Szabo, *supra* note 394.
411 *See generally* Kaunain Sheriff M, *How Johnson and Johnson Hip Implants System Went Wrong*, THE INDIAN EXPRESS (Aug. 30, 2018), https://indianexpress.com/article/explained/johnson-and-johnson-how-hip-implants-went-wrong-jp-nada-5331779/.

directed J&J to pay INR 7.5 lakh compensation to the first patient from Mumbai in 2019.[412]

iii. Scope of Product Liability under Consumer Protection Act, 2019

It is noteworthy that the new Consumer Protection Act, 2019 [*hereinafter* "**CPA**"][413] has specifically incorporated the aspect of product liability. According to Section 2(34) of CPA,[414] "product liability" refers to the responsibility of a product manufacturer or seller to pay compensation for any harm caused to a customer because of any defective product or deficient service. A pertinent question may further arise as to whether ML incorporated into software itself counts as "product" under CPA? Under Section 2(33) of the CPA[415] "product" includes any article or goods or extended cycle of such product, possessing intrinsic value that can be delivered either as wholly assembled or as a component part and produced for commercial purposes.

It appears that the existing definition coupled with the inherent opacity of AI software (as standalone product) may be challenging to establish liability under the CPA. However, if AI software is implemented

---

[412] *See CDSCO Directs Johnson & Johnson to Pay Rs. 74.5 Lakh to First Patient With Faulty Hip Implant*, WIRE (Mar. 13, 2019), https://thewire.in/health/cdsco-directs-johnson-johnson-to-pay-rs-74-5-lakh-to-first-patient-with-faulty-hip-implant.
[413] Consumer Protection Act, 2019, Act No. 35, Acts of Parliament, 2019 (India) ("**CPA**").
[414] CPA, § 2(34).
[415] CPA, § 2(33).

into devices to make it a composite product (*e.g.*, a blood glucose monitor) and it fails, the manufacturer of such product may be held liable.[416]

C. RELEVANCE OF STRICT PRODUCT LIABILITY

It appears that because of the complexity of the AI programmes and difficulty in determining as to where exactly the fault lies, ordinary liability principles may fall short. Yet they hold inherent potential in causing considerable harm. This calls for a special situation, *i.e.*, strict liability, where if the products are defective to a great extent and dangerous, the seller/manufacturer shall bear the responsibility for any loss or personal injury. In such a scenario, the law stipulates a defendant to compensate the claimant's loss even if he was not at fault. Nevertheless, it is not an absolute principle as there may be disclaimers on product liability, a recovery cap, or the economic damage may not be recoverable.[417]

Over the last century, courts have found that proving injury cases against manufacturers and vendors was arduous for critically injured consumer claimants. In *Escola v. Coca-Cola Bottling Co.*,[418] a case where an explosion of a Coca-Cola bottle caused injury, the Supreme Court of California decided in favour of the plaintiff by employing the doctrine of *res ipsa loquitur*. However, in the concurring judgement Justice Roger Traynor observed that instead of relying on the principle of negligence, the manufacturer should have incurred "absolute liability" for placing an article

---

[416] Johan Ordish, *Legal liability for machine learning in healthcare*, PHG Foundation, (Aug. 2018), https://www.phgfoundation.org/media/217/download/briefing-note-legal-liability-for-machine-learning-in-healthcare.pdf?v=1&inline=1.
[417] *See* Ghosh and Ray, *supra* note 403.
[418] *See* Escola v. Coca Cola Bottling Co., 24 C2d 453 (1944).

in the market which he knew would be sold without inspection, and that proved to have a defect causing injuries to others.

Subsequently, in the case of *Henningsen v. Bloomfield Motors, Inc.*,[419] the plaintiff bought a car from the defendant's dealership. The express warranty was only to replace the defective parts. However, the plaintiff's wife met with an accident because the steering had malfunctioned. The plaintiff filed a lawsuit against both the dealer and the auto maker. The defendants declined to pay for repairing the vehicle under warranty because they claimed their warranty only covered defective parts and were not liable for any damage caused by defective parts. The New Jersey Supreme Court rejected this claim and granted Henningsen damages, reasoning that the sale of each item was accompanied by an implicit guarantee of protection.

The principle has received some mentioning in India in the case of *Airbus Industries v. Laura Howell Linton*,[420] where deaths and injuries were caused due to a faulty landing of an aircraft. When the defendants argued that Indian law did not have strict product liability, the Karnataka High Court retorted that merely because Indian courts haven't enunciated such a principle, parties could not go without any remedy. It was observed that if required, a new principles would be brought in to remedy such situations as was done in *Charan Lal Sahu v. Union of India*[421] in the aftermath of the Bhopal Gas Tragedy.

---

[419] *See* Henningsen v. Bloomfield Motors, Inc., 32 N.J. 358 (1960).
[420] *See* Airbus Industries v. Laura Howell Linton, I.L.R. 1994 Kar. 1370.
[421] *See generally* Charan Lal Sahu v. Union of India, A.I.R.1990 S.C.1480.

Although this principle hasn't found a place in the CPA, it deserves mentioning that Section 87 of the Act[422] lays down certain specific exceptions to product liability. However, those exceptions do not specifically address the situations that are being discussed in this paper.

Nevertheless, the application of strict product liability principle to AI can be complicated. In this area, the cause-and-effect relationship, as it relates to the causality of the injury, may not be linear. An AI technology designer cannot necessarily foresee how the technology will act once it is being used in a real-world medical setting. Furthermore, even though there are no bugs in the design or its execution, the results can be unpredictable. As many entities and individuals, such as designers, engineers, and developers, work together to create an AI technology and its systems, it makes it extremely difficult to pinpoint the "fault" and blame any single individual.[423]

There is another downside to imposing strict liability. This could expose producers and programmers to volatile and potentially limitless civil liability lawsuits, with no way to mitigate the risks by raising safety investments because the harm could be unforeseeable. Hence, AI designers could be reluctant to indulge in research to their full potential and it could eventually hamper technological progress.[424]

---

[422] CPA, § 87.
[423] *See* Marchisio, *supra* note 372, at 61.
[424] *See generally id.*, at 62 – 63.

In such a scenario, a possibility arises of conferring AI tools/programmes with a 'legal personality' or in other way treating them as robots.[425] Then such robots will have the legal status compared to human clinicians and may be sued for any damage caused due to their actions. The operator/clinician may opt for compulsory insurance cover so that any claims arising out of its use can be paid out of the insurance. Further, the insurance itself may have a cap so that there is no limitless liability on the insurance company either. However, all this may only be made possible through appropriate legislation in this regard.

V. LIABILITY REGARDING PROTECTION OF PERSONAL HEALTH DATA

As mentioned earlier, there has been a gradual progression to EHRs, which keep health data in electronic form rather than in physical files. Such a trend has aided the massive development of recorded data. It has also raised the concern of the safety and privacy of EHRs. Since data is at the core of AI-driven health systems, a few fundamental concerns about health data ownership, use, and accountability in the event of data misuse or unauthorised use must be addressed. Confidential and private data will be used in AI healthcare applications. There have been cases of substantial violations both in India and abroad which further emphasise the need to fix liability in such situations.

---

[425] *See generally* Mariam Mgeladze and Murman Gorgoshadze, *Applicability of Legal Regulations to High Artificial Intellect - Robots*, 2019 J. Const. L. 51 – 72 (2019).

A. INSTANCES OF VIOLATION OF PATIENTS' DATA

In 2017, a major controversy sparked when London-based Royal Free National Health Service Foundation Trust floundered in adhering to the data privacy laws when it revealed 1.6 million patient records to Google-owned AI firm DeepMind for a trial. Investigation in this matter revealed that as part of the trial, the Trust did not inform patients about the extent of usage of their details. It struck a deal with Google and shared patient's sensitive personal data, *e.g.*, HIV status, mental health history and abortions, without their express consent. The Information Commissioner's Office held that the deal was a serious violation of the right to privacy and ordered for tighter guidelines. However, it did not penalise the Trust financially. Both the Trust and DeepMind admitted the breach and committed themselves to stricter norms.[426]

Recently, a similar data privacy infringement took place in the State of Kerala. The state government contracted with Sprinklr, a US-based tech firm, for the management of personal information of COVID-19 patients, and allegedly gave access to data of 175,000 people of Kerala without their "informed consent".[427] The opposition party in the state called for the cancellation of the agreement and sought the intervention of the High

---

[426] *See* Alexander J Martin, *NHS patients' data was illegally transferred to Google DeepMind*, SKY NEWS (Jul. 7, 2017), https://news.sky.com/story/nhs-patient-data-given-to-google-illegally-10935315.

[427] *See* Anil S, *Sprinklr row: Controversy which blotted the COVID-19 clean slate of Kerala Government*, INDIAN EXPRESS, (Apr. 26, 2020), https://www.newindianexpress.com/states/kerala/2020/apr/26/sprinklr-row-controversy-which-blotted-the-covid-19-clean-slate-of-kerala-government-2135352.html.

Court as such data breach amounts to the violation of right to privacy under Article 21 of the Constitution of India.[428] The High Court also did not appreciate the state's decision for choosing the jurisdiction of the courts in New York and that the agreement was finalized without sanction of the Law Department.[429] In order to ensure that there is no "data epidemic" after the COVID-19 is contained, in an interim order, the High Court in *Balu Goplalakrishnan v. State of Kerala* [*hereinafter* "***Sprinklr case***"] issued certain directions which include:[430]

a) The state government requires individuals to provide informed consent for their data to be handled by a third-party foreign corporation.
b) The state should only allow Sprinklr to access anonymised data.
c) Sprinklr was restrained from exploiting any data for commercial purposes.
d) Sprinklr should respect the confidentiality and return the entire data to the state after its contractual obligations are over.

---

[428] *See Sprinklr Deal: Kerala HC Seeks Govt Explanation on Foreign Jurisdiction Clause and Lack of Law Dept. Sanction*, LIVELAW NEWS NETWORK (Apr. 21, 2020), https://www.livelaw.in/news-updates/sprinklr-deal-kerala-hc-seeks-govt-explanation-on-foreign-jurisdiction-clause-and-lack-of-law-dept-sanction-155559; *see also Balu Gopalakrishnan v. State of Kerala and Ors.*, GLOBAL FREEDOM OF EXPRESSION (COLUMBIA UNIVERSITY), https://globalfreedomofexpression.columbia.edu/cases/balu-gopalakrishnan-v-state-of-kerala-and-ors/.

[429] Balu Goplalakrishnan v. State of Kerala, W.P.(C). Temp. No. 84 of 2020, ¶ 1. ("***Sprinklr case***").

[430] *See id.*, at ¶ 24.

Facing flacks from all corners, the Government of Kerala eventually cancelled the deal with Sprinklr and informed the High Court about the same.[431]

B. DRAWING INSPIRATION FROM EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

The European Union's [*hereinafter* "**EU**"] data protection legal regime, the General Data Protection Regulation [*hereinafter* "GDPR"], is considered as one of the developed data protection models,[432] and it applies to all EU member states as well as all organisations that hold and process personal data about EU residents, regardless of where they live. In other words, GDPR has an impact on data protection requirements globally. Failure to comply with the requirements prescribed under the GDPR attracts stiff penalties to the extent of € 20 million or 4 per cent of the corporation's annual global revenue, whichever is greater. It may also be mentioned that it has served as a model for many countries outside the EU, including India, to draft their own laws.[433]

---

[431] *See generally* Jeeman Jacob, *Kerala Backs Out of Sprinklr Deal, Cancels Controversial Pact Over Privacy Issues*, INDIA TODAY, (May 21, 2020), https://www.indiatoday.in/india/story/kerala-sprinklr-deal-covid-19-pinarayi-vijayan-high-court-1680484-2020-05-21.

[432] *See generally* Lakshya Sharma and Siddharth Panda, *Into the Orwellian Dystopia: A Comparative Analysis of Personal Data Protection Bill 2019 vis-à-vis Indian Privacy Jurisprudence*, 7(2) NLUJ L. REV. 1, 15 – 17 (2021) ("**Sharma and Panda**").

[433] *See generally* Juliana De Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (Sep. 30, 2020), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

The GDPR's core privacy and data protection provisions include the following:[434]

a) No data processing without the subjects' permission;
b) Collected data to be anonymised for maintaining privacy;
c) Notifying data principals about data breaches;
d) Ensuing safety in transferring of data across borders; and
e) Appointment of data protection officers by certain companies to supervise GDPR compliance.

According to a study commissioned by the European Commission, GDPR has a bearing on AI-powered mobile health applications. Accordingly, operating systems and device manufacturers, third parties (*e.g.*, advertisers), mobile-health app developers, etc., must comply with privacy rights and abide by the concept of necessity and proportionality. Use of anonymised data or at least the use of pseudonymised data should be favoured. The use of non-pseudonymised data should be reduced as much as possible.[435]

It highlights that the concept of consent is crucial in healthcare beyond data protection as a component of the patient's self-determination. The study reveals that patients will not normally have access to the application unless they agree to the rules of the mobile health app. Further,

---

[434] *See id.*

[435] *See* C. HOLDER *ET AL.* (EDS.), LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE: THE CASE OF AUTONOMOUS VEHICLES, M-HEALTH AND DATA MINING 19 (2019), https://publications.jrc.ec.europa.eu/repository/bitstream/JRC116235/jrc116235_report_on_ai_%281%29.pdf.

availability of the information only in English creates a hindrance for the patients to give informed consent.[436]

The study report stated that if the AI medical devices are covered under EU Regulation 2017/745 on medical devices, then they are required to conform with CE markings,[437] information duties, etc,[438] making the producers liable for causing any harm; however, it was found most of them are unaware of such regulations.[439] The producer/owner of the AI software/product is forced to adopt a privacy by design approach[440] and would be liable under the GDPR for any breach of privacy. In case the producer and operator are two different entities, the GDPR might fall short. Since GDPR only applies to data controllers and processors, it does not apply to companies who still generate software that processes personal data. In this situation, the producer and operator's current contractual arrangement should be examined. This contract should fix the duties of the producer. Companies using software produced by a third party should highlight the same in their contracts.[441]

---

436 *See id.*, at 20.
437 The CE marking (an acronym for the French "Conformite Europeenne") certifies that a product complies with EU health, safety, and environmental regulations, ensuring safety of consumers. *See Certifying Your Product with CE Marking,* INTERNATIONAL TRADE ADMINISTRATION, https://www.trade.gov/ce-marking (last visited May 31, 2021).
438 *See id.*, at 23.
439 *See id.*
440 The European General Data Protection Regulation 2016/679, art. 25(1).
441 *See id.*, at 24.

C. INDIA: RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION BILL, 2019

Unlike the EU, India lacks an extensive law dealing with personal data security. The Information Technology Act, 2000[442] [*hereinafter* "**IT Act**"] was initially enacted to make internet commerce easier by granting legal status to electronic transactions. However, it was amended in 2008[443] to include, *inter alia*, provisions for protection of data collected, processed or stored electronically.[444] Currently, the data protection regime is governed by the IT Act read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[445] [*hereinafter* "**IT Rules**"] framed under Section 43A of the Act.[446] The legal framework mandates that a "body corporate" must protect "sensitive personal data or information" when providing any service or performing under a contract, adhere to certain standards, and pay compensation to the affected person in the event of a "intentional personal data breach" under Section 72A of the IT Act.[447] Such information includes "medical records and history".[448] The body corporate is obligated to

---

[442] Information Technology Act, 2000, Act No. 21, Acts of Parliament, 2000 (India) ("**IT Act**").
[443] Information Technology (Amendment) Act, 2008, Act No. 10, Acts of Parliament, 2009 (India).
[444] PRS Legislative Research, *Rules and Regulation Review: The Information Technology Rules*, 2011, PRSINDIA (Aug. 12, 2011), https://prsindia.org/files/bills_acts/bills_parliament/2011/IT_Rules_and_Regulations_Brief_2011.pdf.
[445] Ministry of Communications & Information Technology (Department of Information Technology), Notification No. G.S.R. 313(E) (Apr. 11, 2011).
[446] *See* IT Act, § 43A.
[447] *See* IT Act, § 72A.
[448] *See* IT Rules 2011, r. 3.

provide a privacy policy and to be available to the data owner,[449] who shall give informed consent about the purpose for such collection but can withdraw his earlier consent.[450] Although the consequences of such withdrawal are noted under the IT Rules, it can logically be deduced that this will lead to the erasure of data by the corporate.[451] Every corporate is to designate a grievance officer for addressing any discrepancies and grievances expeditiously within one month of their receipt.[452]

The IT Rules further provide that, save in the case of a legal (or statutory) duty, a body corporate must get the prior authorization of the supplier of sensitive personal data before disclosing such data to any third party.[453] Any data processor will be presumed to have complied with the IT Rules if it has met the relevant international standard mentioned therein or its equivalence approved by the Central Government.[454]

Personal health data is part of our right to privacy whose protection has been deliberated in various judgements of the Supreme Court,[455] culminating into *Justice K. S. Puttaswamy (Retd.) v. Union of India*, [*hereinafter* "***Puttaswamy***"][456] where the Court held "right to privacy" as part of the

---

[449] *See id.*, r. 4.
[450] *See id.*, r. 5.
[451] *See* Vinod Joseph, Protiti Basu and Ashwarya Bhargava, *India: A Review of The Information Technology Rules, 2011: Reasonable Security Practices and Procedures and Sensitive Personal Data or Info*, MONDAQ (Mar. 19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-.
[452] *See* IT Rules, 2011, r. 5(9).
[453] *See id.*, r. 6.
[454] *See id.*, r. 8.
[455] *See generally* Sharma and Panda, *supra* note 432, at 18 – 21.
[456] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

right to life and personal liberty as enshrined under Article 21 of the Constitution of India. Although the Supreme Court held that the right is not an absolute guarantee, the invasion of one's privacy whether by a private or public actor must pass the triple test, *i.e.*, (a) legitimate aim, (b) proportionality, and (c) legality. The directions issued by the Kerala High Court in *Sprinklr case* provides further protection to the health data.

Rapid development in technology left many aspects unaddressed through the existing law, and drawing impetus from the GDPR, the Government presented Personal Data Protection Bill, 2019 [*hereinafter* "**PDP Bill**"],[457] before the Lok Sabha on December 11, 2019, and subsequently referred it to the Standing Committee in the pursuit of enacting the legislation.[458] The PDP Bill regulates personal data processing by the government, Indian corporations, and international corporations. As per the PDP Bill, "personal data" refers to information about an individual's features, qualities, or attributes of identity that can be used to classify them.[459] Further, it classifies "health data" as "sensitive personal data".[460]

The PDP Bill allows for a data fiduciary, whether in the case of a natural or legal individual, to process personal data under certain conditions, including purpose, processing, and storage limitations. Personal

---

[457] Personal Data Protection Bill, 2019, Bill No. 373, Bills of Parliament, 2019 (India).
[458] PRS Legislative Research, *The Personal Data Protection Bill, 2019*, PRSINDIA, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019 (last visited May 31, 2021).
[459] *See* Personal Data Protection Bill, 2019, cl. 2(28).
[460] *See id.*, cl. 2(36).

data processing, for example, should not be permitted unless there is a specific, clear, and lawful reason for doing so. Accordingly, the data fiduciaries are obligated towards ensuring transparency and accountability, together with instituting grievance redressal mechanisms dealing with individual complaints.[461] It further requires substantial data fiduciaries that handle sensitive personal data to complete a data security review before proceeding with any procedure involving the use of emerging technology, extensive profiling, or the use of sensitive personal data.[462]

The PDP Bill envisions the data principal having a number of rights, including the right to seek assurance from the fiduciary regarding collection of their personal data, the right to restrict continued disclosure of such data by a fiduciary, data correction and erasure, data portability, and so on.[463] It also aims to clarify different aspects of consent that are relevant for the processing of personal data.[464] The PDP Bill does, however, list the grounds for collecting personal data without permission, which include reacting to any medical emergency arising from a life threat or a serious health compromise of the data subject or any other individual.[465] This gives the state a scope to process our personal health data in situations like the COVID-19.

It is far-fetched to expect citizens in a nation like India, where poverty and illiteracy have completely disenfranchised them, to be able to

---

461 *See id.*, chap. II.
462 *See id.*, cl. 27.
463 *See id.*, chap IV.
464 *See id.*, cl. 11.
465 *See id.*, cl. 12.

secure their personal data from their own government. The PDP Bill appears to assume a mature knowledge of the concepts of privacy and consent, which shows a serious lack of care. Even the most educated members of our society are frequently indifferent to these characteristics.[466] Possibly, large scale awareness programmes, especially emphasizing on safety and privacy, could ease the problem and the COVID-19 pandemic has created the appropriate opportunity. Data processors are required to ensure that data principles are informed adequately about the usage of their data. In the health sector, the clinics/hospitals whoever collects the data should have the informed consent of the patients, otherwise, they would be held liable in case of any illegality.

The proposed law bans the processing of sensitive personal data and critical personal data (as defined by the Central Government) outside of India, without specific consent by the data principal and until the Data Protection Authority approves the processing. A non-obstante clause, on the other hand, functions by allowing an individual or agency involved in health or emergency services to explain the need for prompt action.[467] The PDP Bill also prescribes stricter penalties in case of contravention of its provisions.[468] However, experts have expressed concerns about the open-ended exception clauses. They have emphasised that the Bill significantly

---

[466] *See* Padmini Ray Murray and Paul Anthony, *Designing for Democracy: Does the Personal Data Protection Bill 2019 Champion Citizen Rights?*, 55(21) ECO. & POL. WKLY (2020), https://www.epw.in/engage/article/designing-democracy-does-personal-data-protection (last visited May 31, 2021) ("**Murray and Anthony**").
[467] *See id.*, chap. VII.
[468] *See id.*, chap. X.

simplifies the government's task of processing data in order to compulsorily register its residents, blatantly disregarding *Puttaswamy*'s scope, which allows the government to collect data under limited conditions.[469]

Although there is an emphasis on data localization, experts are not convinced. Their contention is based on the assertion that any security and governmental access do not bear any correlation to localisation of the data. In this hyper-connected technological ecosystem, even though the data is stored within the country, the encryption keys can be out of reach of national authorities, unless the data is stored and accessed over a captive private network.[470]

In fact, data localization is a government mandate that data be stored on servers that are physically situated inside a state's borders. It supports the idea of data sovereignty, in which states have the ability to exercise sovereign control over the internet and internet users within their authority.[471] Proponents of data localization say that it is necessary to ensure data privacy. In practice, mandatory data localization might lead to more government surveillance. For a variety of reasons, it compromises privacy. Data localization, for example, compromises information security by increasing the number of data centres that firms must monitor. Furthermore, data localization restricts our service providers to those that

---

[469] *See* Murray and Anthony, *supra* note 466.
[470] *See* Kamal Taneja and Gulshan Rai, *Data Protection Bill is Vague and Intrusive,* HINDU BUSINESS LINE (Mar. 15, 2020), https://www.thehindubusinessline.com/opinion/data-protection-bill-is-vague-and-intrusive/article31075785.ece.
[471] Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L. J. 328, 360 – 63 (2018).

operate locally; experience shows that protectionism affects the quality of a service.[472] Madhulika Srikumar and Bedavyasa Mohanty have accused the Justice B.N. Sreekrishna Committee, mandated to create a national privacy regime, for unconvincingly pushing for data localization. They argue that the Committee's assertation in anticipation of a strong Indian claim in case of accessing of data is a weak one, and dependent on bilateral agreements with entities in countries where our data is stored.[473] However, the same has found its way in the PDP Bill.[474] Stringent procedural norms with regard to providing foreign entities with data is the need of the day. The *Sprinklr case* controversy reminds us that the fears are not completely unfounded.

VI. CONCLUSION

Considering the nature of AI health tools available today, mostly under human supervision, the *res ipsa loquitur* doctrine may lessen the victim's hardship in proving the factum of negligence in case of injuries suffered due to the usage of such tools, yet bigger challenges lie ahead. Due to the inherent nature of opacity in their decision-making, determination of liability among manufacturer, operator or clinician precisely, it is still challenging in many cases. While joint-liability could be a temporary solution, it cannot be a long-term and comprehensive answer. Law would

---

[472] *See* Anupam Chander, *Why Democrats and Republicans Should Oppose Data Localization,* COUNCIL ON FOREIGN RELATIONS (Jul. 20, 2016), https://www.cfr.org/blog/why-democrats-and-republicans-should-oppose-data-localization.

[473] *See* Madhulika Srikumar and Bedavyasa Mohanty, *Data localisation is not enough*, THE HINDU (Aug. 3, 2018), https://www.thehindu.com/opinion/op-ed/data-localisation-is-not-enough/article24584698.ece.

[474] *See* Personal Data Protection Bill, 2019, cl. 37.

require assistance from technology in developing explainable AI which would help the judicial authorities to understand the rationale behind arriving at a specific decision of the tool and then identify where exactly the 'fault' lies.

Further, as witnessed in the Tesla incident, despite the fact that the self-driven cars failed to deliver up to the expectation and gave a false sense of comfort and reliability among the victims, NTSB did not hold Tesla strictly liable for the accidents. The J&J fiasco further illustrates that without stricter approval processes, medical devices have the potential in wreaking havoc.

With an increasing number of AI health tools coming to flood the market in the days ahead, CDSCO must gear up for the challenge of examining and approving AI health devices. The concept of strict product liability is yet to find a niche in our jurisprudence, even if it finds no mention under the new CPA. A legislation or an amendment to the law in this regard would be a welcome move. While dealing with such complicated and potentially dangerous AI tools, owners/clinicians may be mandated to take insurance which may have a compensation cap in case of any injury. However, that would not preclude the right of the patient-victims to approach the civil courts for further compensation. As we continuously strive to improve upon the AI tools that would be able to take more complicated decisions without or with minimal human interference, we would be trekking into the difficult terrains of liability regime. Hence,

incorporating the concept of legal personality for the AI tools appears to be the way forward.

The importance of the protection of personal health data in the AI ecosystem is undeniable, yet in such a vast and diverse country with fragmented networks, effective protection of the data is an uphill task. As the majority of healthcare is in private hands, it is a matter of grave concern as to how the commercial interest of the data processors inside and outside the health sector would eventually play.

Despite the fact that the Personal Data Protection Bill, 2019 has laid emphasis on the consent of data principals, the author holds scepticism over whether the majority of the patients will actually be able to give "informed consent" over their data processing. Further, considering the wide nature of the language used for the processing of personal data envisioned in the PDP Bill under the pretext of dealing with medical emergencies, there is ample scope for data compromise. The *Sprinklr case* only reinstates that scepticism. While we wait in anticipation for the PDP Bill to be signed into law, safeguarding personal health data is to be of paramount significance. The dust is yet to settle.