Chettinad Health City Medical Journal
Volume 13, Issue 1 - 2024, Pg. No. 102-107
Peer Reviewed & Open Access Journal

Perspective

Artificial Intelligence in Digital Therapeutics: Exploring the Tangled Web of Legal Issues

Vidya Menon

Assistant Professor, School of Law, SRM IST, Kattankulathur, Tamil Nadu.
DOI: https://doi.org/10.24321/2278.2044.202418

INFO

E-mail Id:
vidyamenon08@gmail.com
Orcid Id:
https://orcid.org/0000-0002-0855-2788
How to cite this article:
Menon V. Artificial Intelligence in Digital Therapeutics: Exploring the Tangled Web of Legal Issues. Chettinad Health City Med J. 2024;13(1):102-107.

Date of Submission: 2023-06-03
Date of Acceptance: 2023-09-02

INTRODUCTION

The increasing penetration of Artificial Intelligence (AI) technologies has transformed the healthcare ecosystem, making it more efficient, accessible and affordable. In recent years, AI-driven technologies have established immense value in the digital diagnosis and treatment process. AI-enabled imaging and digital diagnostic techniques have facilitated early intervention and treatment of critical conditions such as cancer, heart disease, and diabetes. With the ability to quickly learn and analyse large amounts of health data, AI-based techniques have shown tremendous results in delivering more accurate diagnoses, thereby assisting medical professionals in clinical decision-making.[1] The COVID-19 pandemic has also accelerated the adoption of AI-powered remote patient monitoring platforms that connect doctors to patients. In the past three years, as many as 308 AI-enabled medical devices have been either cleared or approved by the United States Food and Drug Administration (US FDA) (Figure 1). It has also been estimated that the healthcare market valuation of global AI shall surpass USD 200 billion by 2030 (Figure 2).

The emerging AI tools are transforming the existing health data management systems into 'smart' electronic health record systems which display patient-specific medical records as and when the clinician needs them, thereby saving a lot of time, which is otherwise spent in navigating these systems.[2] In fact, the adoption of electronic health records (EHR) has been extremely beneficial when it comes to maintaining up-to-date patient data, enabling quicker access to patient records, and providing reliable sharing of patient health information. The development of specific AI-based models has also been helpful in predicting neurodegenerative diseases such as Alzheimer's and dementia, at least 5 years in advance.[3] Similarly, AI has been responsible for the evolution of robotic surgery, which has showcased admirable success rates, ranging between 94% and 100%.[4] Designed to work with enhanced precision and control, these AI-assisted robots have proved to be a priceless asset for the medical fraternity, positively affecting innumerable lives worldwide.

AI-based machine learning techniques have been developed to accurately quantify the blood flow to the heart muscle, evaluate the medical condition using new automated imaging techniques and predict the chances of heart attacks in patients.[5] AI technologies have also been helpful in the diagnosis and management of stroke, which still remains one of the leading causes of mortality across the globe, with an annual morbidity rate of 5.5 million.[6] Lung cancer is one of the deadliest cancers as 70% of the cases are detected in the advanced stages. However, a recent study revealed lung cancer detection accuracy of 93% using AI tools.[7] According to the World Health Organization, the number of deaths owing to cardiovascular diseases is close to 17.9 million each year.[8] A correct and early diagnosis enhances the chances of performing effective treatments, thereby improving survival rates.

However, just like any powerful tool, there are several risks and unintended consequences associated with the application of AI tools in the healthcare sector. The risk of bias, lack of clarity in automated decision-making, trust and security issues, the accountability factor especially in imputation of liability, privacy concerns, and lack of comprehensive regulatory framework are some of the major challenges that need to be addressed urgently. The article highlights the intricate web of legal issues associated with the use of AI technologies in digital therapeutics and the complex road ahead.

AI Black Box Issue in Healthcare Space

The human brain consists of billions of neurons which communicate with each other and work together, taking on the responsibility of regulating bodily functions. Similar to a human brain, artificial neural networks comprise nodes, each of which receives input from one or more other nodes or external sources. Each node contains three layers, namely, the input layer, the hidden layer and the output layer. The data, which first enters the input layer is processed in the hidden layer, and the result is transmitted through the output layer. The internal logic on which the hidden layer processes the data is private to the neural network such that the obtained results may sometimes be incomprehensible. In understanding the working of AI systems, the individuals therefore tend to limit their scope of understanding to the inputs provided into the system and the output it generates. The process by which Artificial Intelligence Systems (AIS) determine the output is thus often compared to a black box; sufficiently complex and beyond ordinary human interpretability.[9] Even though the AI applications designed to work with exceptional accuracy are gradually transforming the healthcare landscape, the alleged opacity (popularly known as the AI black box issue) and lack of transparency and accountability raise some serious and justifiable concerns. The black box functionality in AIS hinders the clinicians from evaluating the quality of outputs that are generated and their decision-making, which may consequently violate the patients' autonomy and their right to informed consent.[10]

Machine learning is a branch of AI that makes use of data and algorithms to replicate the human learning process; whereas a deep learning system (a subset of machine learning) is an enormous artificial neural network, with numerous hidden layers, having the capacity to recognise patterns and learn on its own. Machine learning approaches can be broadly classified into two – supervised and unsupervised. Supervised machine learning algorithms are often based on a wide range of sample data fed into the system that trains it to process the data, identify the patterns and predict the pre-defined outcomes with minimum error. Unsupervised learning models, on the other hand, do not involve a pre-defined outcome and are used to discover, identify and infer patterns and trends in the unlabelled data, on their own.[11] While these techniques can save a lot of time and analyse the data more accurately, these methodologies can also pick up hidden biases which are often difficult to detect. Systemic data biases may be on account of factors such as the absence of complete data, lack of data diversity, use of misrepresentative sample data or employment of data collection techniques which are significantly influenced by human subjectivity.[12] Biased data may result in flawed diagnosis and improper delivery of care which may adversely affect patient outcomes. One of the biggest concerns of machine learning models is that they offer very little visibility on their inner working such that, even the makers find it rather challenging to identify the biases and devise strategies to address them.[13]

Advancements in AI have also paved the way for robotic surgeries that assist surgeons in performing complex tasks with enhanced precision. Robotic surgery that utilises machine learning data and algorithms is revolutionising the field of surgery. However, this may add new complexities, especially in affixing accountability, culpability and liability. Despite the growing trends towards the adoption of robotic surgery, the technical difficulties and complexities experienced during the process cannot be overlooked.

ISSN: 2278-2044
DOI: https://doi.org/10.24321/2278.2044.202418

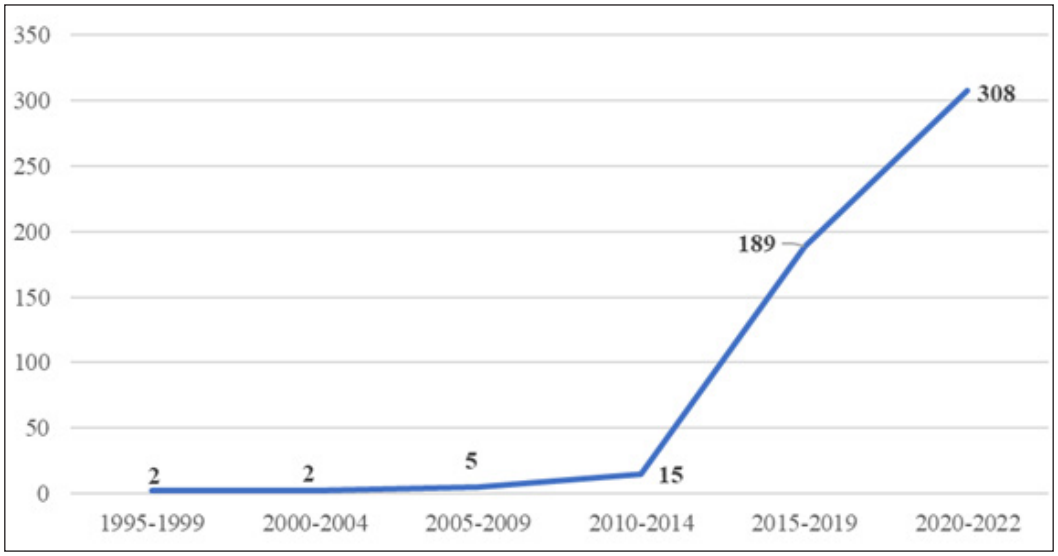

Figure 1.AI/ ML-Enabled Medical Devices Cleared/ Approved by the FDA (1995–2022)[14]

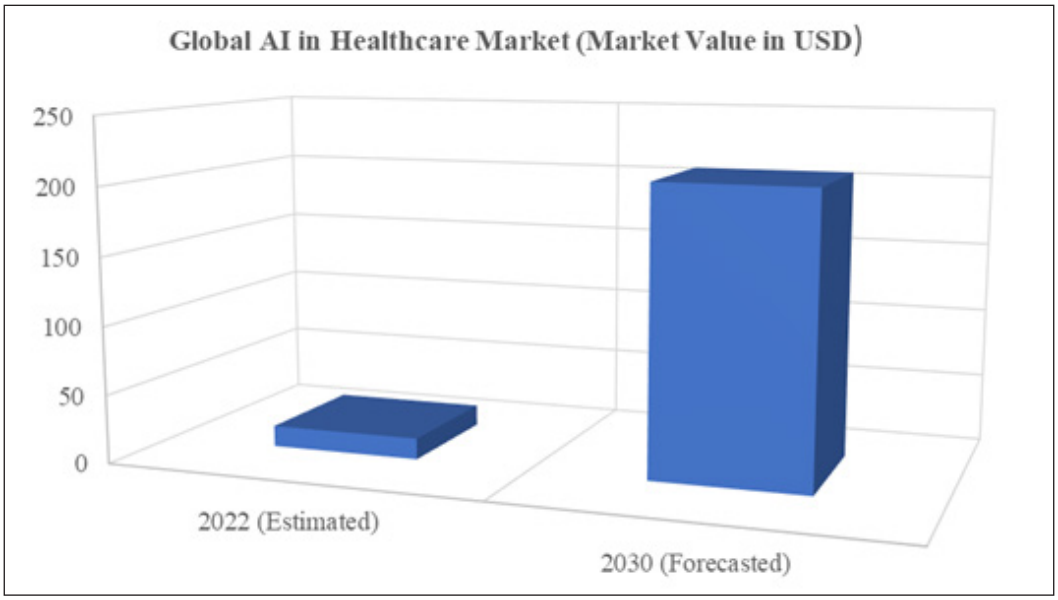

Figure 2.Global AI in Healthcare Market (Market Value in USD)[15]

AI Accountability and Challenges in Imputation of Liability

Until the emergence of AI-based technologies in the healthcare space, clinicians were solely responsible for their recommendations and decision-making based on patient diagnosis and evaluation. However, the development of AIS has altered the clinical relationships in a manner that technologists, clinicians or even AI-assisted systems can jointly and severally be held accountable for patient care. However, very often we come across situations where clinicians have little idea about how the AIS system operates; technicians, though equipped to aid the clinicians, are unavailable in the decision-making space and AI-driven applications, though developed to provide an accurate assessment and treatment of a patient, are prone to system malfunction and errors. In such an instance, the pertinent question to be addressed is who shall be held liable for the clinical decision-making, based on the AIS output that is generated. If we do not hold the people accountable, are we creating an unsafe environment for the patient community? Accountability creates a sense of responsibility for the creators/ developers and promotes trust among the users. However, when it comes to the use of AI applications in healthcare, it is difficult to ascertain the responsibility as it often involves the contributions of multiple persons. Despite its complexities, it is essential to affix the responsibility for the use of AI in the healthcare space as the absence of it allows mistakes to flourish, creating a huge gap in the system.

ISSN: 2278-2044
DOI: https://doi.org/10.24321/2278.2044.202418

Though attempts are made to overcome the present crisis by designing explainable AIS models that are comprehensible and transparent, currently there are no specific laws that regulate the use of AI. In determining the liability, the standard norm has been to ascertain whether the person could reasonably foresee the outcome and if so, did they intend to cause the particular outcome. The severity of the penalty is often based on the intent of the concerned parties and the degree of harm caused in any given situation. However, when it comes to the use of AI-driven technologies in the healthcare sector since the machines and computer programs are said to possess no intent, we may have to assess the intent of the creators or the clinicians. But, if a system functions outside what the creators could reasonably predict, or if a clinician in good faith acts as per the outcomes predicted by the AIS, consequently causing any harm to the patient, the intent theory cannot be relied upon.[16] Since AI systems are a product of many choices made by those who develop and deploy them, it may be difficult to apply the general principles of imputation of liability.

Security and Privacy Concerns in Health Data Management

AI-based applications in the healthcare sector have gained significant attention in recent times, particularly in the context of enhancing the quality of patient care delivery. In developing algorithms for machine learning and thereby effectively assisting clinicians with the process of diagnosis and treatment, these tools often utilise large volumes of patient data. The entire procedure involving the collection, storage and processing of health data has generated significant focus on the considerable risk that it poses to patient data security and privacy. Data forms the basis of almost all AI applications and it plays a crucial role in recommending personalised treatments and preventive care solutions for patients. The strain of a pandemic has accelerated the rise in smart medical devices, accessories and applications which offer a range of benefits for both users and healthcare providers. In this era where digital transformation is reshaping the healthcare sector, ensuring the privacy and security of healthcare data becomes very critical.

AI-Assisted Wearable Devices

Most of the IoT-enabled medical devices and healthcare apps which are commonly used today, come with an advanced set of features wherein real-time patient data can be collected, stored, analysed as well as shared with clinicians. AI-assisted wearable technological devices such as fitness trackers, and smart health watches, which enable the users to keep track of the number of steps walked, the calories burnt, heart rate, blood pressure, oxygen saturation, duration of sleep etc. have gained a lot of popularity lately. According to recent reports, the use of wearable technologies is likely to flourish over the next few years and will result in a considerable reduction in global healthcare costs, as well as clinician-patient interaction time.[17]

While these technologies play a rather motivational role in assisting the users to set and achieve fitness goals and thereby take active steps to maintain a healthy routine, the bigger concern relates to the ownership and appropriate use of the abundant data that gets generated. The sensitive patient information which is collected through these devices may additionally be stored in the company's storage system. If that is the case, who holds the ownership of the data? Would it be the company or the user? In the absence of effective laws and regulations relating to wearable technologies, the user is left with no remedy, especially in instances involving data breaches or identity theft arising out of such AI-driven innovations. There is no legal obligation for the manufacturers of wearable technologies to review the cybersecurity vulnerabilities or provide timely security patches and updates, which makes the entire aspect of the regulation quite challenging.

Smart Pill Technology

Another promising AI-based technological innovation that has evolved as an integral component of remote patient monitoring, is the smart pill technology. Medication non-adherence is a serious concern that can result in adverse consequences. The World Health Organization (WHO) in its report on medication adherence emphasised how enhancing the effectiveness of patient medication adherence may have a much greater impact on public health in comparison to any advancement in specific medical treatments.[18] Smart pill technology has been developed with an aim to address the issues pertaining to medication non-adherence, optimise treatment management and thereby improve patient outcomes.[19] Embedded with a digital tracking system, the smart pills are designed to perform advanced functions such as sensing, imaging and drug delivery.[20] 'Abilify MyCite,' the first digital pill to have been approved by the US, was introduced to treat patients suffering from serious mental illness (such as schizophrenia, bipolar disorder or massive depressive disorder), by helping them to take their medications as directed.[21]

The smart pill technology not only aids in remote monitoring of patients but also offers a sneak peek at the user's lifestyle and behaviour. The digital intervention enhances the risk of healthcare data breaches, putting patient privacy in peril. There is a lack of certainty as to who, apart from the user and the doctor-in-charge, could possibly have access to the patient data. Since the data gathered by the networked system belongs to the patient, they shall have a definitive right to make informed choices as to who may access this

ISSN: 2278-2044
DOI: https://doi.org/10.24321/2278.2044.202418

information. However, the ideal situation of empowering the patients to be in the driver's seat, may not happen at all times due to various factors. The absence of effective data management systems, inherent cybersecurity weakness of the device systems and deficiency of appropriate legal framework that applies to EHR are factors that can result in potential abuse of confidential data, consequently violating the aspect of patient privacy.

Though there aren't any specific legislations pertaining to the regulation of AI-enabled medical devices, there is a wide range of laws dealing with the protection of sensitive patient data and health information. Health Insurance Portability and Accountability Act (HIPAA) 1996, is one such legislation which was passed by the U.S. Congress to ensure the availability, confidentiality and integrity of 'protected health information' (PHI), 'electronic protected health information'(e-PHI) and 'personally identifiable information'(PII). In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was introduced to encourage healthcare providers to adopt EHR systems and thereby strengthen the privacy and security goals under HIPAA. However, one of the present-day challenges is that HIPAA applies only to a 'covered entity' and does not essentially extend its scope to the data collected or generated by some of these modern wearable technologies and healthcare applications. Likewise, the General Data Protection Regulation (GDPR) was implemented in 2016 to protect the personal data and privacy of the citizens and residents in the EU. Considered to be more stringent than HIPAA, GDPR prohibits the processing of any health data unless it is expressly allowed by law or the individual has explicitly consented to it. Even though, GDPR and similar laws modelled after GDPR (such as the Personal Data Protection Act (Thailand), the Data Protection Act (the UK), and the Personal Information Protection Act (South Korea)) attempt to partly regulate the AI systems by safeguarding the individuals against solely automated decision making, it does not afford a comprehensive protection against the risks associated with emerging AI systems.

Conclusion

AI is transforming all walks of life and one of the biggest challenges in formulating any regulatory mechanism for AI is that it must be proportional to the risk and must be balanced to encourage innovation. Concerns about the potential misuse and the devastating effects such unregulated technologies can have on human lives, have prompted us to develop appropriate standards and laws that provide for trustworthy AI systems. However, due to the immense intricacies, legislators across the globe have remained unsuccessful in designing comprehensive legislation that effectively regulates AI. The primary goal of AI is to benefit mankind and make our lives easier and more convenient. In the larger interest of society, what we need today is a regulatory regime that keeps pace with technological advancements and ensures that emerging technologies benefit humanity as a whole.

With the aim of building robust and reliable AI systems, recently, the EU has proposed the enactment of the AI Act, which could set new global standards for the regulation of AI. The Act, which is modelled on a risk-based approach, classifies the AI systems into four categories – unacceptable risk, high risk, limited risk and minimal risk. The rigour of the regulation shall be proportional to the level of risk and further requires the providers to set up a risk management system for the entire lifecycle of the AI system. Amidst growing concerns about the AI black box algorithmics in decision-making, as well as the security and privacy of patient health information, this shall be the first-ever attempt globally to comprehensively regulate such AI-based systems.[22]

There have also been several initiatives taken by the countries at the national level to encourage the adoption of responsible AI. These include the 'National Artificial Intelligence Research and Development Strategic Plan' launched by the U.S. government, 'New Generation Artificial Intelligence Ethics Specifications,' the 'Ethical Principles for Artificial Intelligence Development' and the 'Guiding Opinions on Regulating the Development and Application of Artificial Intelligence' released by the Chinese government, the 'Pan-Canadian Artificial Intelligence Strategy', an initiative by the government of Canada, 'the AI National Strategy' established by the Korean government, 'National Strategy for Artificial Intelligence, formulated by NITI Aayog, the think tank of government of India, in India etc. AI is transforming the future of the healthcare landscape globally and such governmental initiatives focus on reaping the benefits of deploying AI in a manner that is responsible to the users as well as the society. Responsible AI works towards creating systems that minimise unintended bias, ensure transparency and ultimately develop solutions that are sustainable in the long run.

Conflict of Interest: None

Source of Funding: None

References

1. Bates DW, Levine D, Syrowatka A, Kuznetsova M, Craig KJ, Rui A, Jackson GP, Rhee K. The potential of artificial intelligence to improve patient safety: a scoping review. NPJ Digit Med. 2021;4(1):54. [PubMed] [Google Scholar]
2. Serbanati LD. Health digital state and smart EHR systems. Inform Med Unlocked. 2020;21:100494. [Google Scholar]

3. PTI [Internet]. AI may predict Alzheimer's disease 5 years in advance. The Hindu; 2018 Oct 8 [cited 2022 Dec 23]. Available from: https://www.thehindu.com/sci-tech/health/ai-may-predict-alzheimers-disease-5-years-in-advance/article25160303.ece
4. Schwaibold H, Wiesend F, Bach C. The age of robotic surgery – is laparoscopy dead? Arab J Urol. 2018;16(3):262-9. [PubMed] [Google Scholar]
5. National Heart, Lung and Blood Institute [Internet]. Researchers use artificial intelligence to help predict heart attacks and strokes; 2020 Feb 14 [cited 2022 Dec 28]. Available from: https://www.nhlbi.nih.gov/news/2020/researchers-use-artificial-intelligence-help-predict-heart-attacks-and-strokes
6. Liebeskind DS. Artificial intelligence in stroke care: deep learning or superficial insight? EBioMedicine. 2018;35:14-5. [PubMed] [Google Scholar]
7. Chiu HY, Chao HS, Chen YM. Application of artificial intelligence in lung cancer. Cancers (Basel). 2022;14(6):1370. [PubMed] [Google Scholar]
8. World Health Organization [Internet]. Cardiovascular diseases; 2021 [cited 2022 Dec 8]. Available from: https://www.who.int/health-topics/cardiovascular-diseases#tab=tab_1
9. Smith H. Clinical AI: opacity, accountability, responsibility and liability. AI Soc [Internet]. 2021 [cited 2022 Dec 16];36:535-45. Available from: https://link.springer.com/article/10.1007/s00146-020-01019-6 [Google Scholar]
10. Fenech M, Strukelj N, Buston O. Ethical, social and political challenges of artificial intelligence in health [Internet]. Future Advocacy Report for the Wellcome Trust; Apr 2018 [cited 2022 Dec 17]. Available from: https://wellcome.ac.uk/sites/default/files/ai-inhealth-ethical-social-political-challenges.pdf
11. Alanazi A. Using machine learning for healthcare challenges and opportunities. Inform Med Unlocked [Internet]. 2022 [cited 2022 Dec 18];30:100924. Available from: https://www.sciencedirect.com/science/article/pii/S2352914822000739 [Google Scholar]
12. Norori N, Hu Q, Aellen FM, Faraci FD, Tzovara A. Addressing bias in big data and AI for health care: a call for open science. Patterns (N Y). 2021;2(10):100347. [PubMed] [Google Scholar]
13. Duran JM, Jongsma KR. Who is afraid of black box algorithms? On the epistemological and ethical basis of trust in medical AI. J Med Ethics [Internet]. 2021 [cited 2022 Dec 16];47(5):329- 35. Available from: https://jme.bmj.com/content/47/5/329
14. US Food & Drug Administration [Internet]. Artificial intelligence and machine learning (AI/ML)-enabled medical devices; 2022 Oct 5 [cited 2023 May 29]. Available from: https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices
15. Business Wire [Internet]. Global artificial intelligence in healthcare market (2022 to 2030) - size, share and trends analysis report - ResearchAndMarkets.com; 2022 Jul 20 [cited 2023 May 27]. Available from: https://www.businesswire.com/news/home/20220720005496/en/Global-Artificial-Intelligence-in-Healthcare-Market-2022-to-2030---Size-Share-and-Trends-Analysis-Report---ResearchAndMarkets.com
16. Bathaee Y. The artificial intelligence black box and the failure of intent and causation. Harvard J Law Technol. 2018;31(2):889-938. [Google Scholar]
17. Vijayan V, Connolly JP, Condell J, McKelvey N, Gardiner P. Review of wearable devices and data collection considerations for connected health. Sensors (Basel). 2021;21(16):5589. [PubMed] [Google Scholar]
18. Brown MT, Bussell JK. Medication adherence: WHO cares? Mayo Clin Proc. 2011;86(4):304-14. [PubMed] [Google Scholar]
19. Chevance A, Fortel A, Jouannin A, Denis F, Mamzer MF, Ravaud P, Sidorkiewicz S. Acceptability of and willingness to take digital pills by patients, the public, and health care professionals: qualitative content analysis of a large online survey. J Med Internet Res. 2022;24(2):e25597. [PubMed] [Google Scholar]
20. Beriain IM, González MM. 'Digital pills' for mental diseases: an ethical and social analysis of the issues behind the concept. J Law Biosci. 2020;7(1):lsaa040. [PubMed] [Google Scholar]
21. Shewalkar SK, Kothwade SM, Patil RA. Digital pills: impact of rising technology. Arch Med. 2021;13(6):26.
22. Lilkov D. Regulating artificial intelligence in the EU: a risky game. Eur View. 2021;20(2):166-74. [Google Scholar]

ISSN: 2278-2044
DOI: https://doi.org/10.24321/2278.2044.202418