Magnetic Resonance Materials in Physics, Biology and Medicine (2020) 33:217–219
https://doi.org/10.1007/s10334-019-00821-8

EDITORIAL

ESMRMB Round Table report on "Can Europe Lead in Machine Learning of MRI-Data?"

Francesca B. Pizzini[1] · Filippo Pesapane[2,3] · Wiro Niessen[4,5] · Liesbeth Geerts-Ossevoort[6] · Nils Broeckx[7,8]

Published online: 3 January 2020

Artificial intelligence (AI) is based on the possibility of collecting, analyzing and integrating multiple data and it aims to interpret complex data, potentially resolve possible apparent contradiction and to reveal solutions. Its application can improve diagnosis, prognosis, be of assistance to patients and it can impact positively on all the expressions of medical care. But the identification of medico-legal rules and regulations—that can guarantee appropriate and safe use of AI in the medical field—is required for exchanging all the information which are essential for safe progress of AI. Surely, one of the forefronts of the digital era in medicine is radiology, and in particular MRI, and the European Union (EU) can play a fundamental role in guiding ethical and legislative statements, but some premises, clarifications and distinctions must be made before proposing a future strategy.

This was the aim of the ESMRMB RT discussion.

1. The state of Art of European, USA and China regulations.

   There are currently no specific regulations on AI in any of these jurisdictions. It appears that the current trend in the USA is to rely on self-regulation by industry against the legal background of the privacy provisions from the Health Insurance Portability and Accountability Act (HIPAA) and the FDA-regulated framework for medical devices. This has led to call for more government-led regulations. In China, the government has already issued a set of ethical principles and is now quickly steering towards AI-specific regulations that must give businesses confidence to venture into AI, potentially making China the leading AI country. The EU strategy is similar to that of China. Following the advice of the European Economic and Social Committee, the High-Level Expert Group on AI presented its Ethics Guidelines for Trustworthy Artificial Intelligence on 8 April 2019. The next step is AI-specific European legislation. Until then, the General Data Protection Regulation (GDPR) and the European framework on medical devices remain the primary regulations that define the legal boundaries of AI development and clinical use.
2. One of the main problems that the EU faces is caused by the intrinsic heterogeneity of the different health care systems and of related national directives that can weaken the strength of a community strategy and of common solutions. Other important issues to deal with are the protection, the security and privacy of the data, liability regarding the clinical use of AI and the type of anonymization of the data, as specified below.

   - In addition to the traditional *data security issues* such as hacking, the processing of data through AI also presents some new risks. Someone could, e.g., maliciously feed the AI with false data and thus disturb the process of machine learning ('poisoning'). These security issues must first be addressed to create trust in medical AI amongst the patient population.

     In the EU, regulators updated the legislation concerning data protection and cybersecurity substituting the European legal framework for data protection as set out by Directive 95/46/EC with the GDPR. A

✉ Francesca B. Pizzini
francesca.pizzini@aovr.veneto.it

[1] Radiology, Department of Diagnostic and Public Health, Verona University, Verona, Italy

[2] Postgraduation School in Radiodiagnostics, Università Degli Studi di Milano, Milan, Italy

[3] IEO, European Institute of Oncology IRCCS, Milan, Italy

[4] Erasmus MC-University Medical Centre Rotterdam, Rotterdam, The Netherlands

[5] Imaging Physics, Faculty of Applied Sciences, Delft University of Technology, Delft, The Netherlands

[6] MR Neuro Imaging, Philips Healthcare, Best, The Netherlands

[7] Dewallens and Partners Law Firm, Leuven, Belgium

[8] PR2 Research Group, Faculty of Law, University of Antwerp, Antwerp, Belgium

frequently heard opinion is that the GDPR requires all data processing and use to be opt-in, and that consumer consent for data use should be clear, prohibiting in that way the current data marketing based on third-party personal data obtained without opt-in. The GDPR is definitely a more suitable instrument to regulate AI, because it has an extended territorial scope and wider rights for data subjects.

The black box features of deep learning and the lack of transparency regarding how results are obtained have thorny legal implications—considering the current amount of data collected and that with an increased presence of AI applications this can only grow, so regulatory actions regarding cybersecurity will face continuous challenges. However, before using government over-regulation, we need to face the cybersecurity implications technologically, because data protection can no longer rely on current technologies that allow the spread of personal data at a large and uncontrolled scale.

- Both healthcare culture and law (such as the GDPR) require physicians to closely protect patients' health data, but the development of large patient datasets incorporating wide ranges of clinical, imaging data and pathologic information across multiple institutions for the development of AI algorithms will necessitate a thorough re-examination of issues surrounding patient *privacy*, confidentiality, and informed consent.
- Although the evolving complexity of AI technology makes it inevitable that some of its inner workings will appear to be a black box, that does not remove the obligation to act *ethically*. Since the AI ecosystem will play an increasingly important part in healthcare, it will need to be bound by the core ethical principles, such as beneficence and respect for patients, which have guided clinicians during the history of medicine. According to the panelists of the RT, ethical and legal responsibility for decision making in healthcare will remain a matter of the natural intelligence of physicians. From this viewpoint, it is probable that the multidisciplinary AI team will take the responsibility in difficult cases, where AI will provide an important, but not exclusive input to the final decision.
- One could avoid the GDPR privacy issues in machine learning altogether by training AI on anonymous data, since the GDPR does not apply to anonymous data. *Anonymization* is however very difficult due to a very strict interpretation of this legal concept. If the AI security issue could however be addressed appropriately, then this would be a strong argument to adopt a more flexible interpretation in line with the so called 'risk-based approach' contained in the GDPR.

3. Future perspectives

- It was discussed during the round table that explicit consent (opting-in) is not the only way to lawfully process personal data for the purpose of machine learning. For example, the GDPR also allows data processing without prior consent if such data processing is necessary to ensure high standards of quality and safety of medical AI devices (art. 9(2)(i) GDPR). Given the data subject's right to object the data processing under the GDPR, this approach would come down to an *opting-out regime*, similar to the presumed consent system for postmortem organ donation. Both themes are based on a balance between the needs of society and the interests of the individual. The opting-out approach for machine learning currently relies on an interpretation of the law, whereby priority is given to the interests of society. This interpretation will only get enough support if the AI is trustworthy, i.e., secure.
- Although the potential of AI is well known in the radiology community, policy makers are now facing a choice: to downgrade the enthusiasm regarding the potential of AI in everyday clinical practice, or to resolve issues of data ownership and trust and *invest in the data infrastructure or/and in models* to realize it, otherwise the opportunities that AI offers to medical imaging (and to medicine in general) will remains just opportunities.
- It was stressed throughout the round table that ensuring security of AI and defining security standards must be one of the main focal points prior to creating AI-specific legislation. It would nevertheless already be useful to further define the legal concept of 'anonymization' like in the USA (through the system of removing identifiers mentioned in the HIPAA). As far as the panelists know, there is no currently available *certification* for tools and methods for *anonymization* and it is difficult to estimate when a general certification can be expected. The great challenge and difficulty in the evaluation of anonymization is that no known method can guarantee 100% data protection. If data are made anonymous, its information content is inevitably reduced and distorted. To ensure that raw data retain their significance in an analysis, the data can only be changed to a certain extent.
- As a final and practical take home message, researchers should encourage their scientific and clinical societies to provide *guidelines and recommendations* for adopting and using medical AI reliability, safely and effectively.

Compliance with ethical standards

Conflict of interest The authors declare that they have no competing interests.

Ethical standards This article does not contain any studies with human participants or animals performed by any of the authors.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.