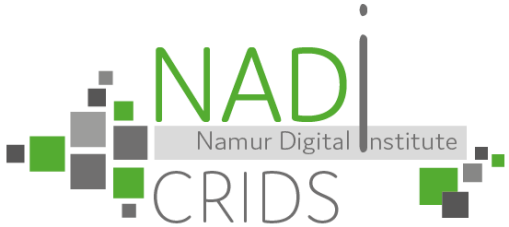
What control for AI systems in personalised medicine?

Noémi Bontridder, Researcher at CRIDS, NaDI, University of Namur

Interdisciplinary seminar *Maths and society*, 27-28 June 2024

Palais des académies, Bruxelles



Agenda

- The use of digital biomarkers in neurological conditions
- Human control requirements under the General Data Protection Regulation
- Further human control requirements under the Artificial Intelligence Act
- Conclusions and broader considerations

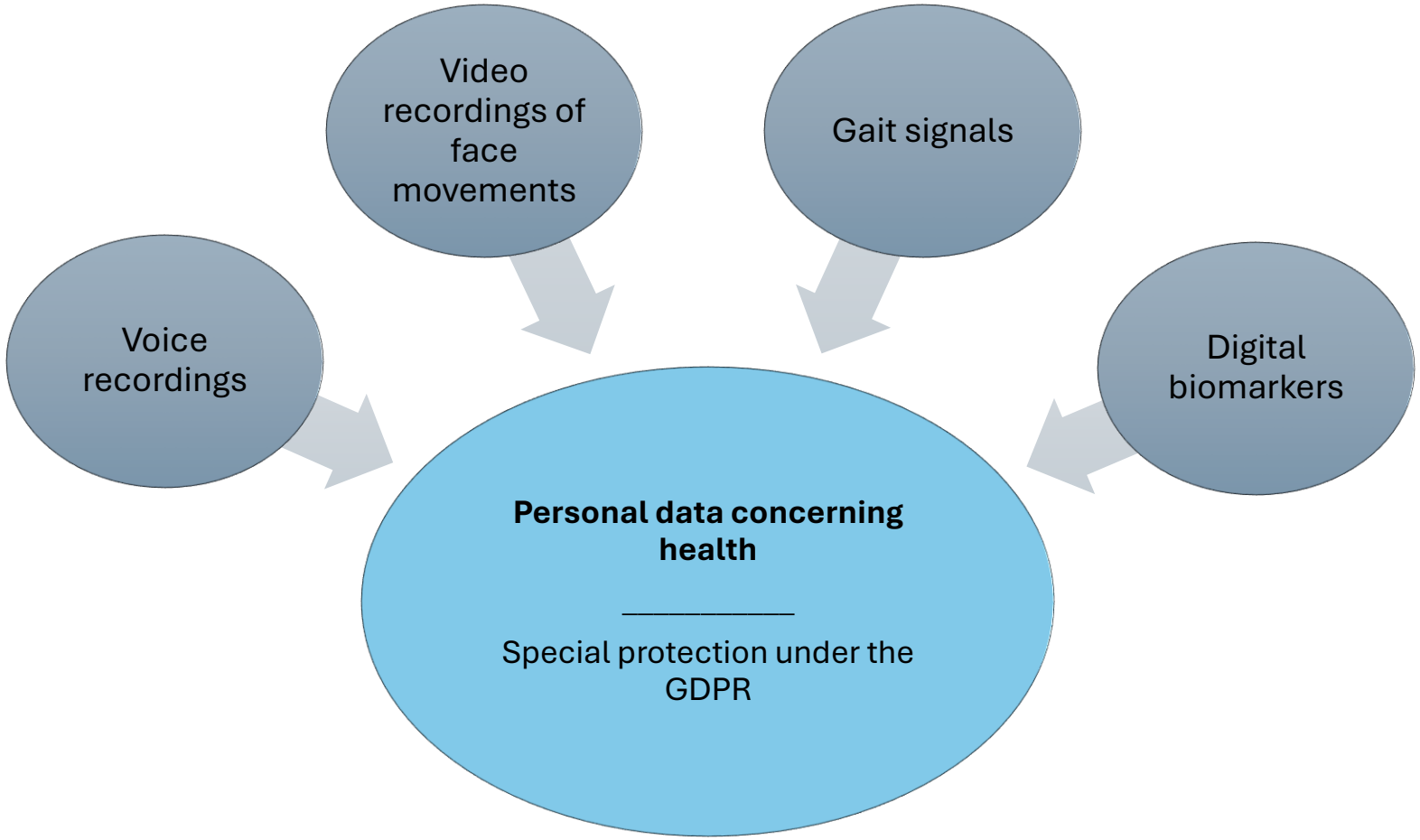
The use of digital biomarkers in neurological conditions

- **Biomarker:** “defined characteristic that is measured as an indicator of normal biological processes, pathogenic processes, or biological responses to an exposure or intervention, including therapeutic interventions”.
- **Digital biomarker:** emerging class of biomarker, where the term ‘digital’ refers to the method of collection as using sensors and computational tools.

- digital biomarkers for speech and voice impairments can be extracted from voice recordings;
- digital biomarkers for hypomimia – or reduced facial dynamics – can be extracted from video recordings;
- and digital biomarkers for gait impairments can be extracted from gait signals.

Automatic extraction is possible using deep learning methods.

The digital biomarkers can be used as inputs for machine learning algorithms to **detect the disease** or to **stratify the patients into different groups**.


Video recordings of face movements
Gait signals
Voice recordings
Digital biomarkers
Personal data concerning health
Special protection under the GDPR

Human control requirements under the General Data Protection Regulation

- **Accuracy of personal data**

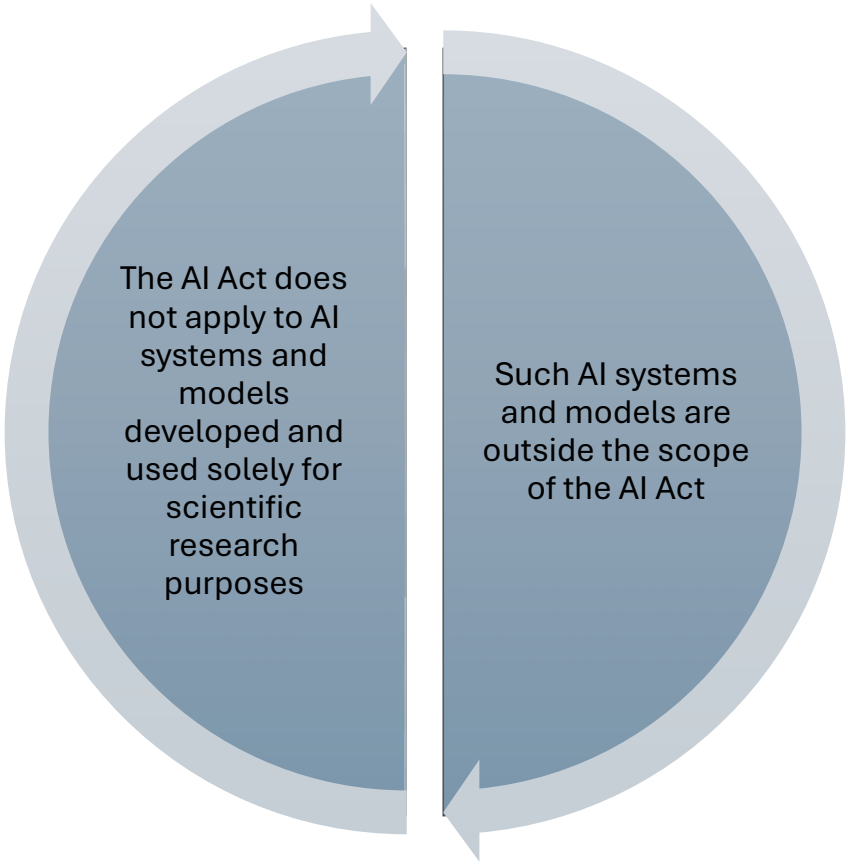
- *Be able to '**provide a copy**'* of personal data

- **Prohibition of solely automated individual decision-making**

- Be able to provide **meaningful information about the logic involved**

a) in the processing operations → **prohibition** of the use of advanced analytical methods for personalised medicine when the logic involved in the *processing* itself cannot be explained (in a concise, transparent, intelligible and easily accessible form, using clear and plain language).

b) in the decision → **possibility** to use digital biomarkers and advanced analytical methods in healthcare only as long as the physician is taking herself the diagnostic or treatment decisions affecting the patient without relying on the output taken out of context: (s)he can explain the reason behind the *decision* (in a concise, transparent, intelligible and easily accessible form, using clear and plain language).


The AI Act does not apply to AI systems and models developed and used solely for scientific research purposes
Such AI systems and models are outside the scope of the AI Act

AI-based medical devices required to undergo a third-party conformity assessment pursuant to Regulation (EU) 2017/745 on medical devices, with a view to their placing on the market or putting into service

= **high-risk AI systems pursuant to the AI Act**

active devices intended to allow direct diagnosis or monitoring of vital physiological processes

software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes

Further human control requirements under the Artificial Intelligence Act

- The system must be "*designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use*".
- The oversight measures must enable '*natural persons to whom human oversight is assigned*':

✓ to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, also in view of detecting and addressing anomalies, dysfunctions and unexpected performance;

✓ to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias');

✓ **to correctly interpret the high-risk AI system's output**;

✓ to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system.

The healthcare professional must be able to correctly interpret the system's output '*for informed decision making*', in accordance with the data protection and healthcare rules.

An explainability algorithm can be specifically developed and used for providing explanations of the system's output.

Conclusions and broader considerations

- If the '*logic involved*' in the processing itself of personal data as well as all personal data, including digital biomarkers, must be explained, advanced analytical methods may not be usable in medical practice.
- If explaining the reason behind the decision suffices, using advanced analytical techniques in personalised medicine may be allowed to better understand characteristics of disease trajectories, or even to identify the potential disease trajectory of an individual patient
  ← as long as the healthcare professional correctly interprets the system's output, takes herself the decisions affecting the patients and meaningfully explains these decisions.

"While biomarkers provide clear opportunity and increased dimensionality of data sources, the increased array of sensors and, thus, data capture needs to be carefully considered against the broader healthcare aims, including sustainability and societal heuristics or behaviours displayed [by] the public. AI is likely to aid in the processing and understanding of complex data, however ***increasingly there is broader ecosystem challenges that need to be addressed in parallel****. Just because 'we can, doesn't mean we should' is an essential reminder of frugality in the face of innovation.* ***Increased 'sensing' and data capture have potential unintended negative impacts of data junk, storage and ultimately environmental impacts***"
(Dylan Powell, 2024)