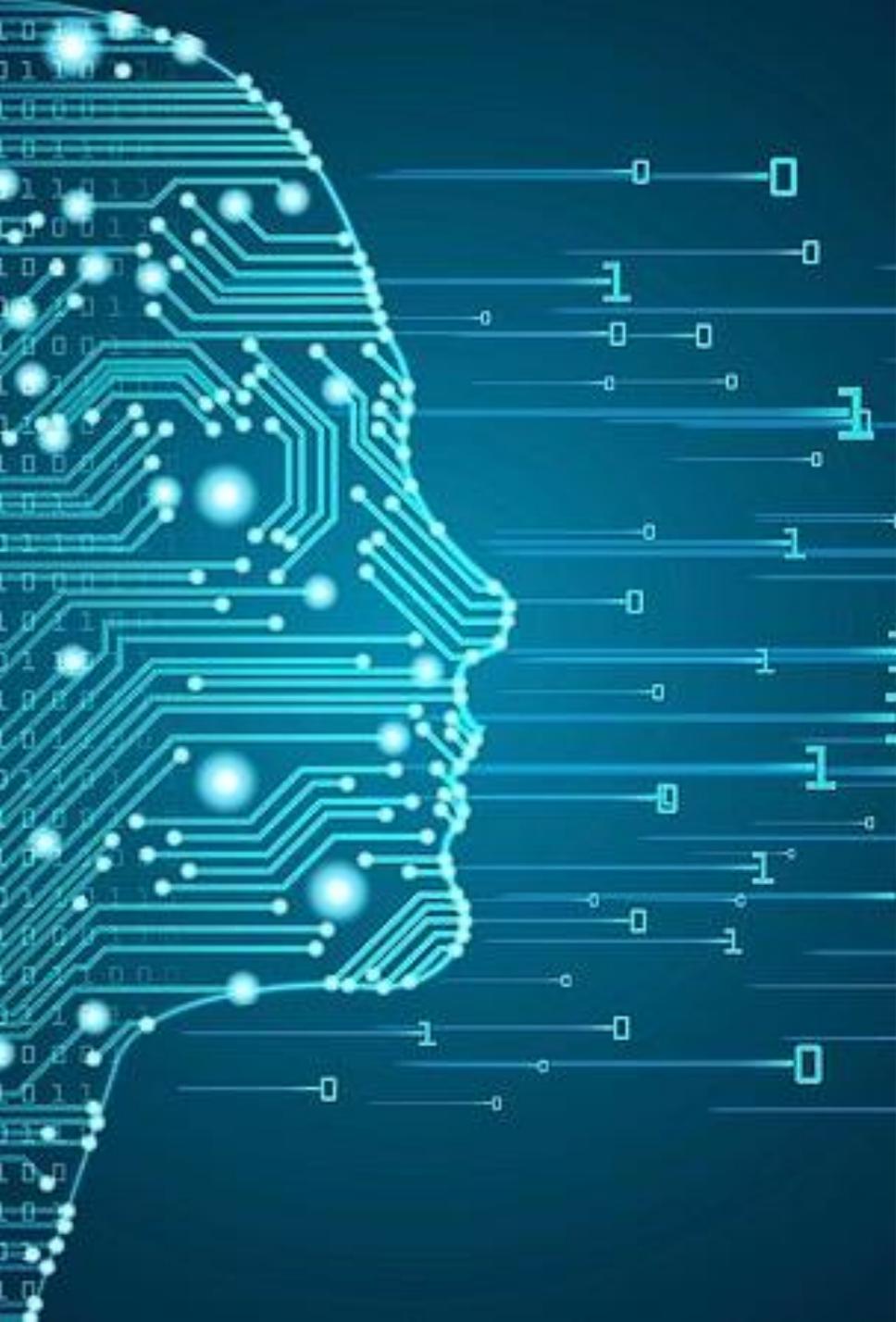# Regulatory Sandboxes

22 November 2022
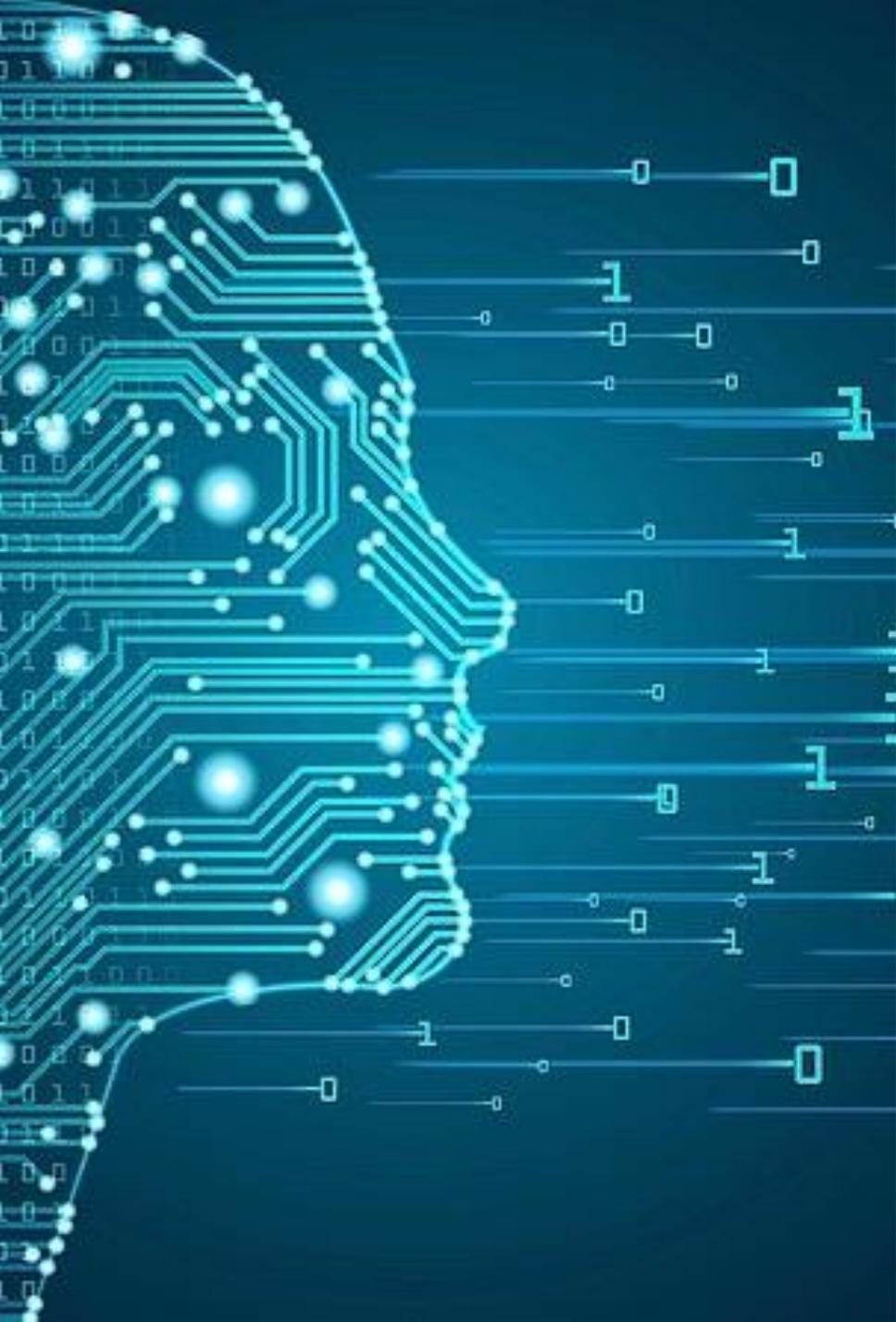
Regulatory experimentation in regulatory sandboxes
differ widely, but
common characteristics:
- temporary,
- they bring together regulators and firms;
- require multi-stakeholder and multidisciplinary cooperation
- test innovative products/services
- **they waive existing legal provisions**
- often based on trial-and-error;
- can help regulatory authorities assess whether specific legal frameworks are fit-for-purpose or whether they need to be adapted.
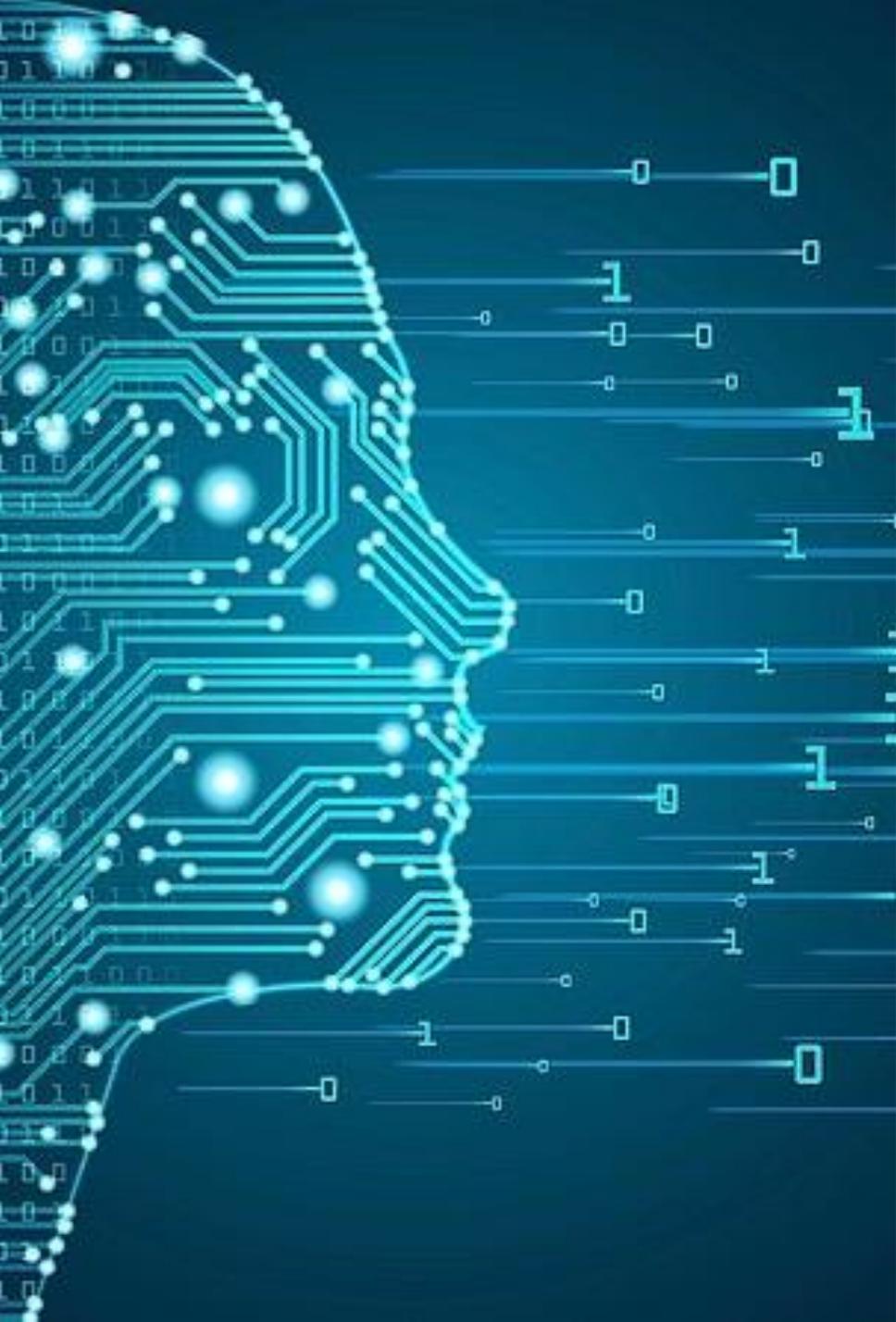
First launched in domain of Fintech

At least 100 initiatives around the world (Fintech, Privacy and AI)

Need for enhanced international co-operation and coordination on regulatory experimentation mechanisms & sandboxes. OECD AI Principle 2.3
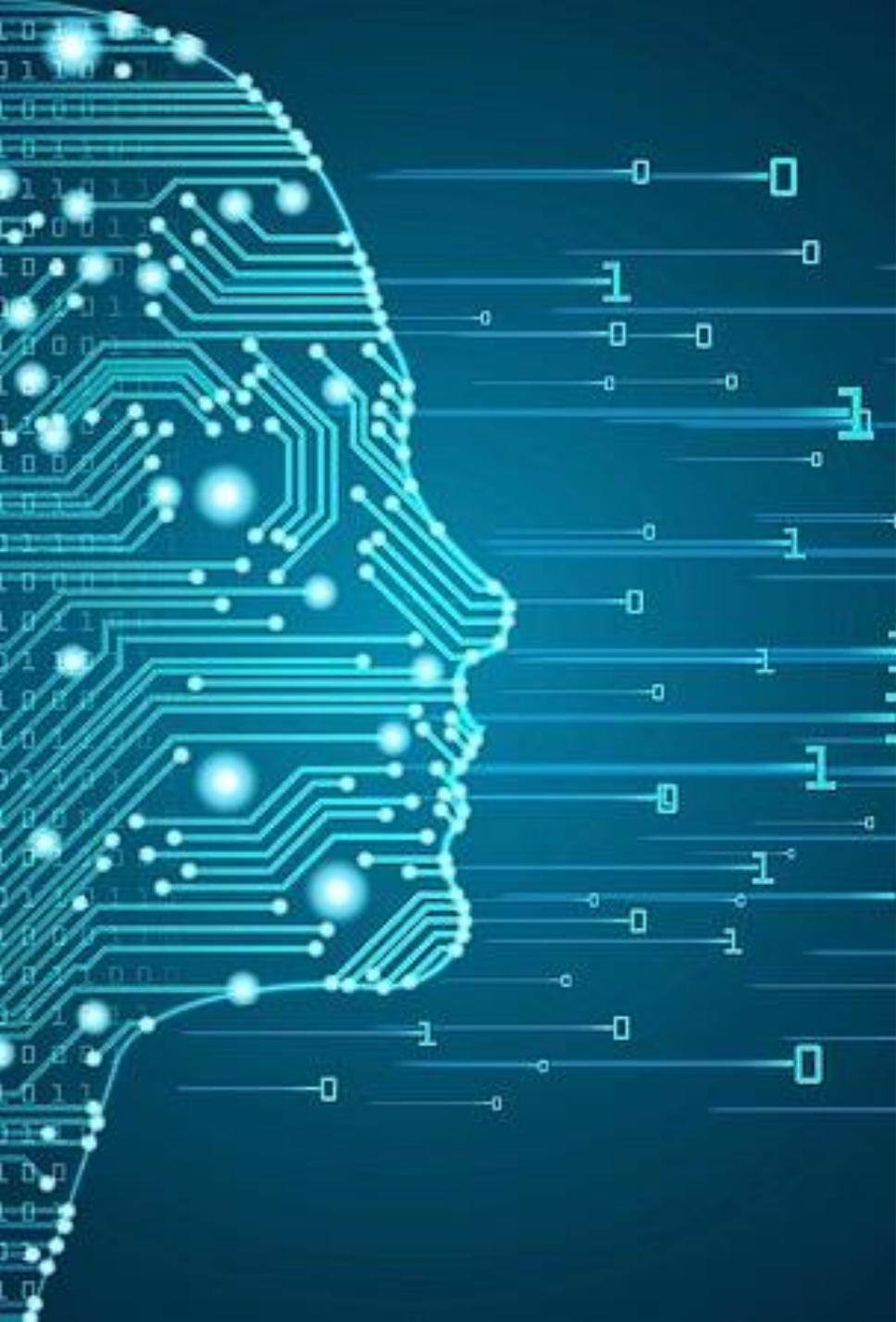
AI Act includes provisions for Regulatory Sandboxes.

AI ACT:
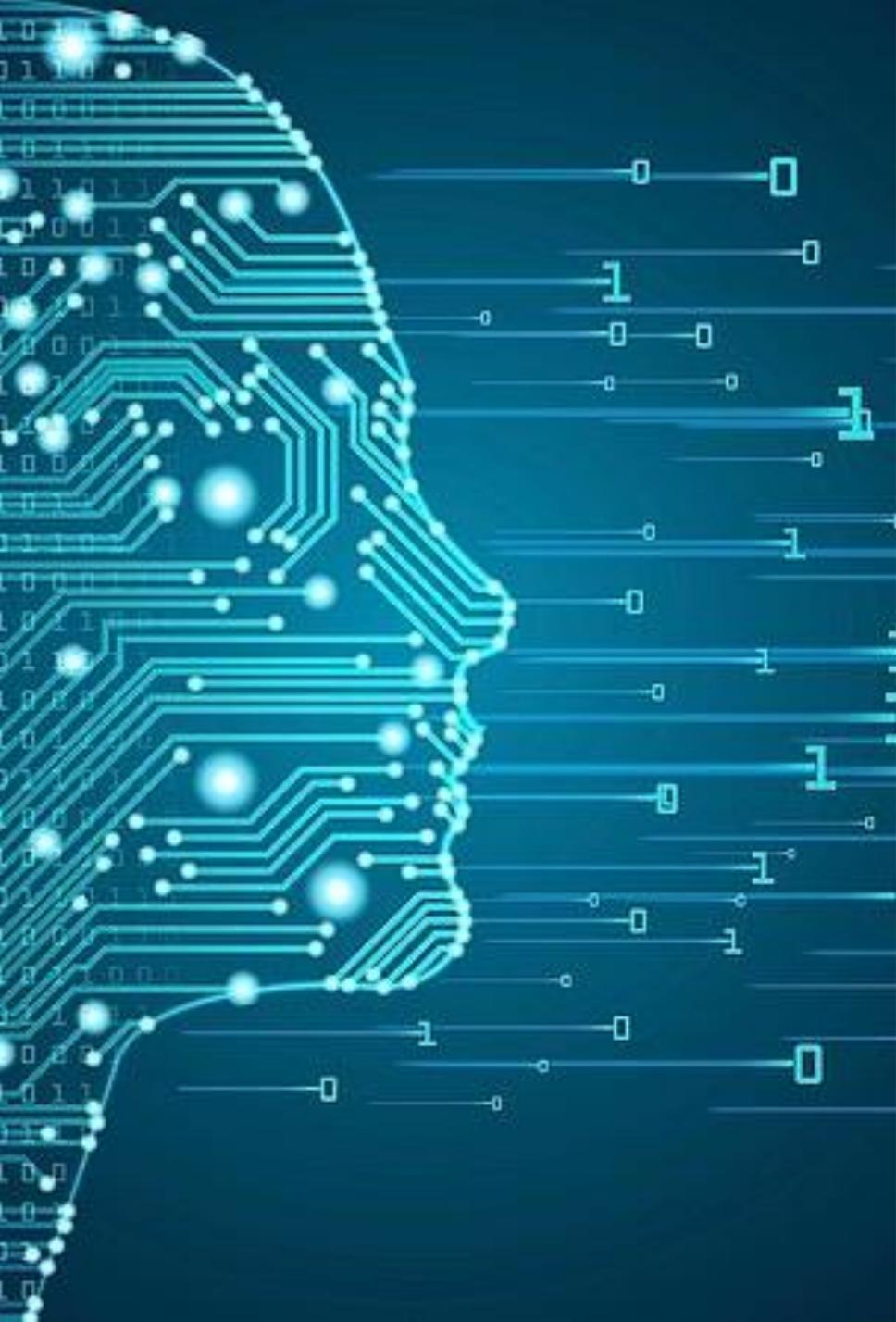# TITLE V MEASURES IN SUPPORT OF INNOVATION
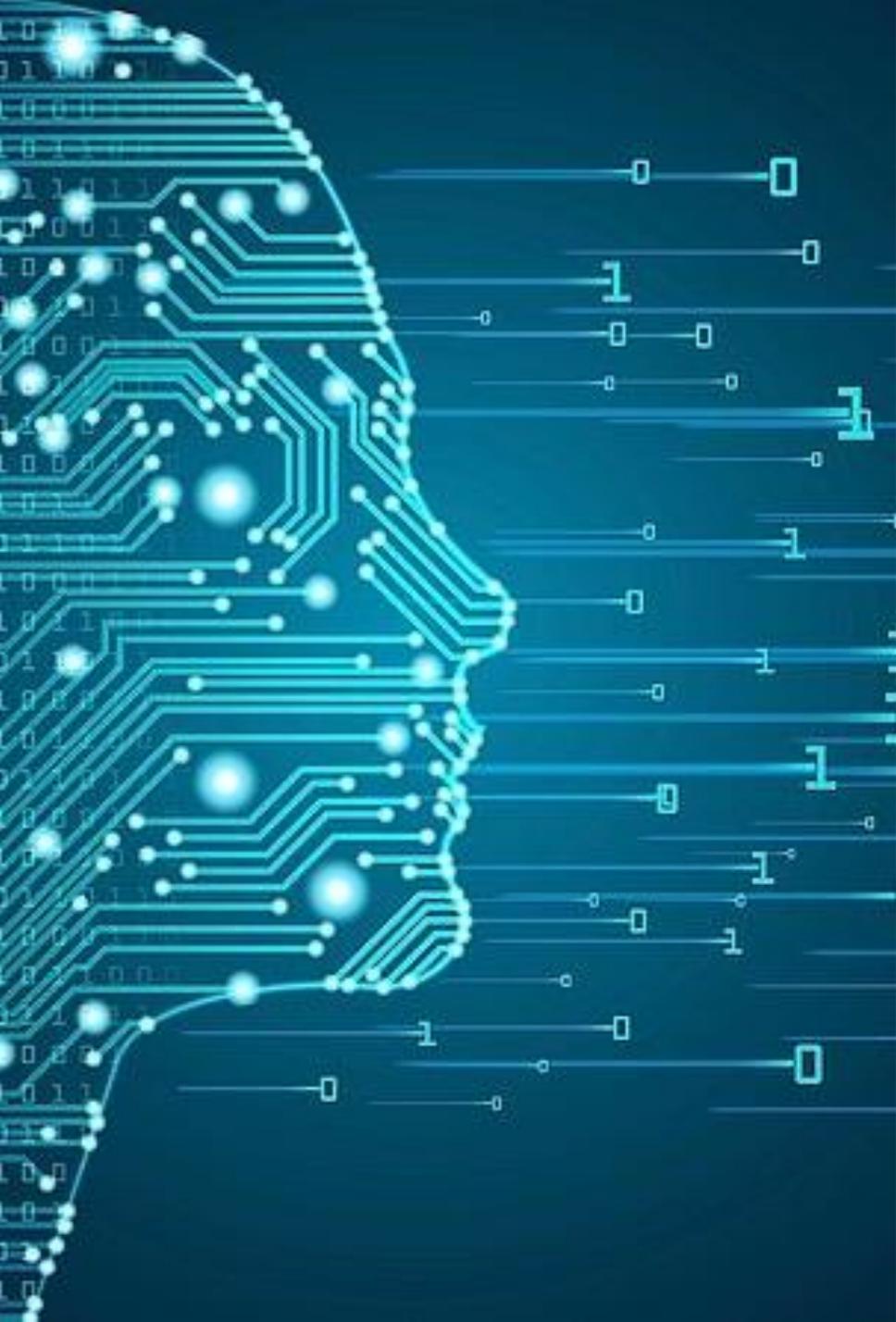
Article 53 AI regulatory sandboxes

Foster **innovation** and **regulatory learning** and shall particularly take into account the special circumstances and capacities of participating SMEs, including start-ups.

The establishment of AI regulatory sandboxes shall aim to contribute to one or more of the following <u>objectives</u>:

a) foster **innovation** and **competitiveness** and facilitate the development of an AI ecosystem;

b) **facilitate and accelerate access to the Union market** for AI systems, in particular for SMEs;

c) improve **legal certainty** and contribute to the sharing of **best practices**

d) contribute to evidence-based **regulatory learning**

2a. Access to the AI regulatory sandboxes shall be open to **any provider** or prospective provider of an AI system [....]

Voluntary basis
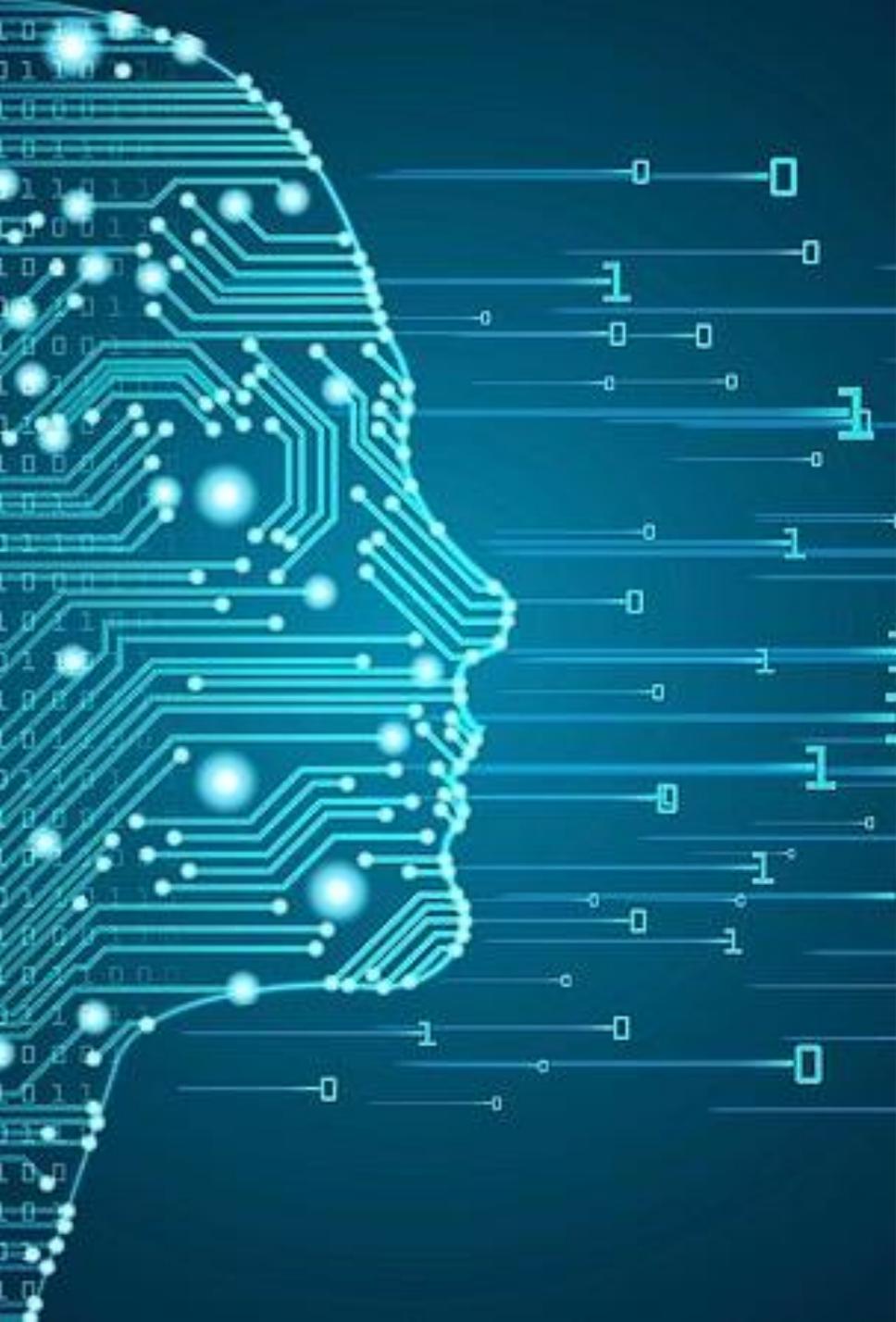
Original proposal European Commission:

Art. 53 paragraph 3

The AI regulatory sandboxes <u>shall not affect the supervisory and corrective powers of the competent authorities</u>.

Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in <u>immediate mitigation</u> and, failing that, in the suspension of the development and testing process until such mitigation takes place.
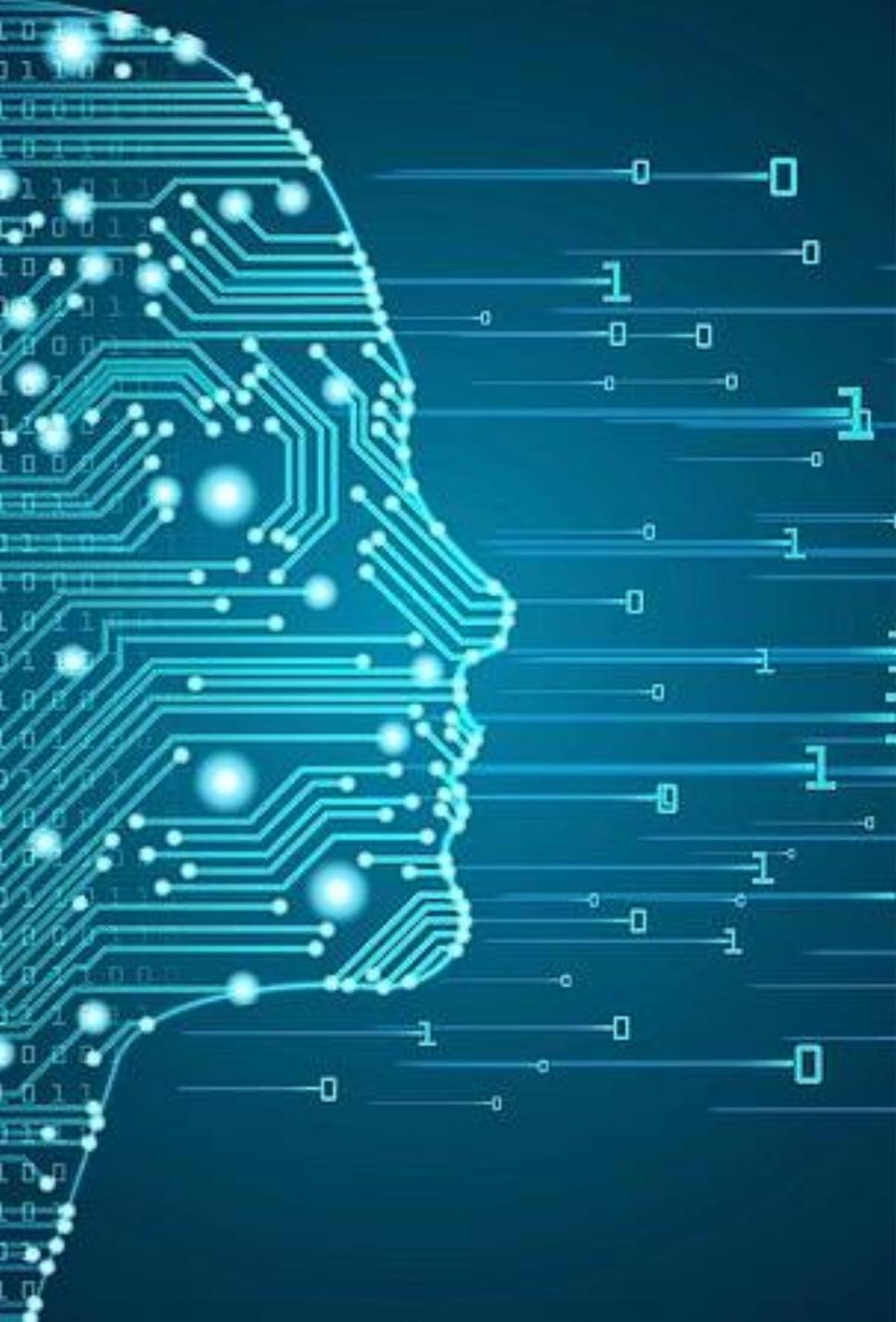
Proposal Council:

Art. 53 paragraph 3

The participation in the AI regulatory sandboxes shall not affect the supervisory and corrective powers of the authorities supervising the sandbox.
Provided that the participant(s) respect the sandbox plan and the terms and conditions for their participation as referred to in paragraph 6(c) and follow in good faith the guidance given by the authorities, <u>no administrative fines </u>shall be imposed by the authorities for infringement of applicable Union or Member State legislation relating to the AI system supervised in the sandbox, including the provisions of this Regulation.
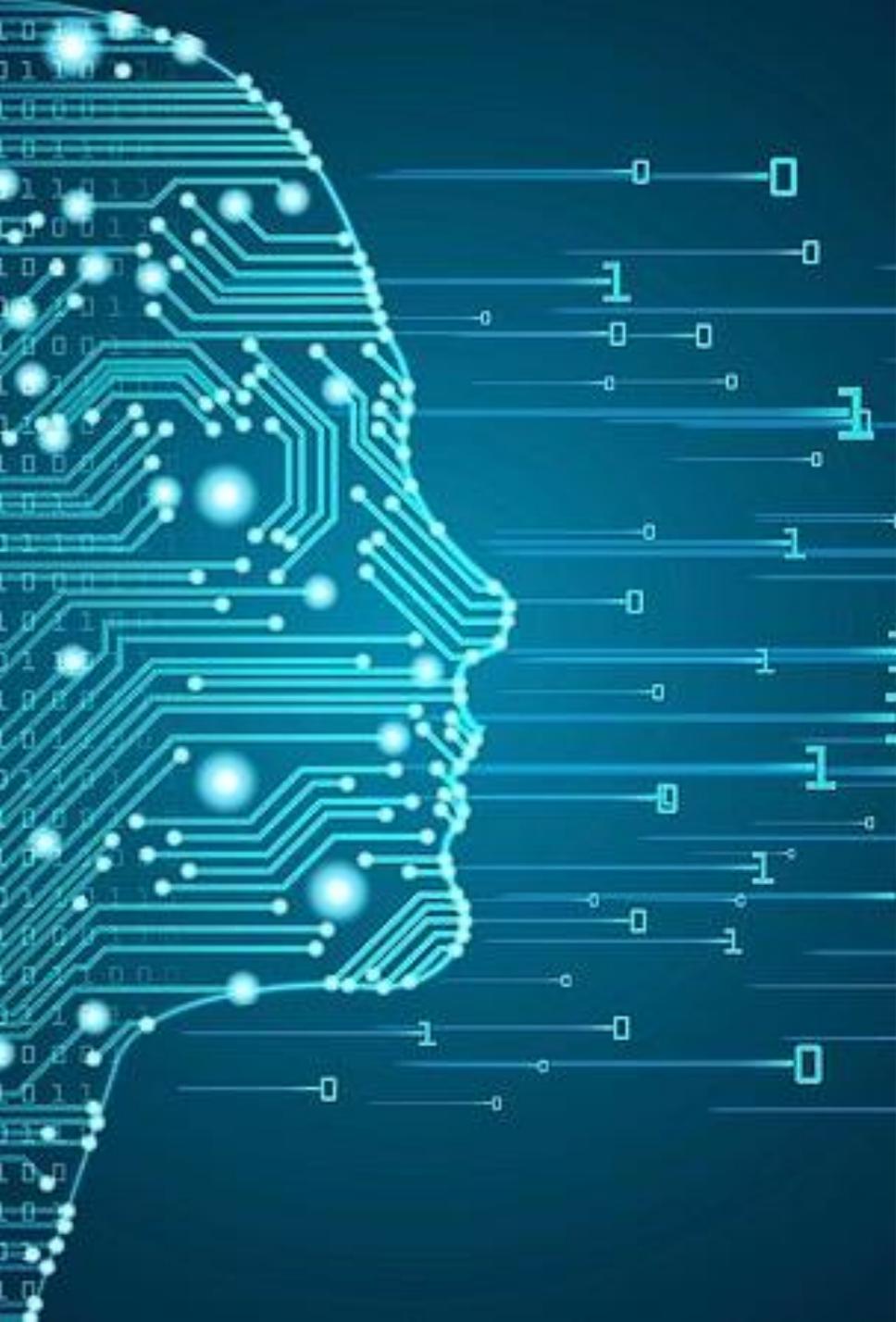
Proposal EP (under construction):

Article 53
AI regulatory sandboxes
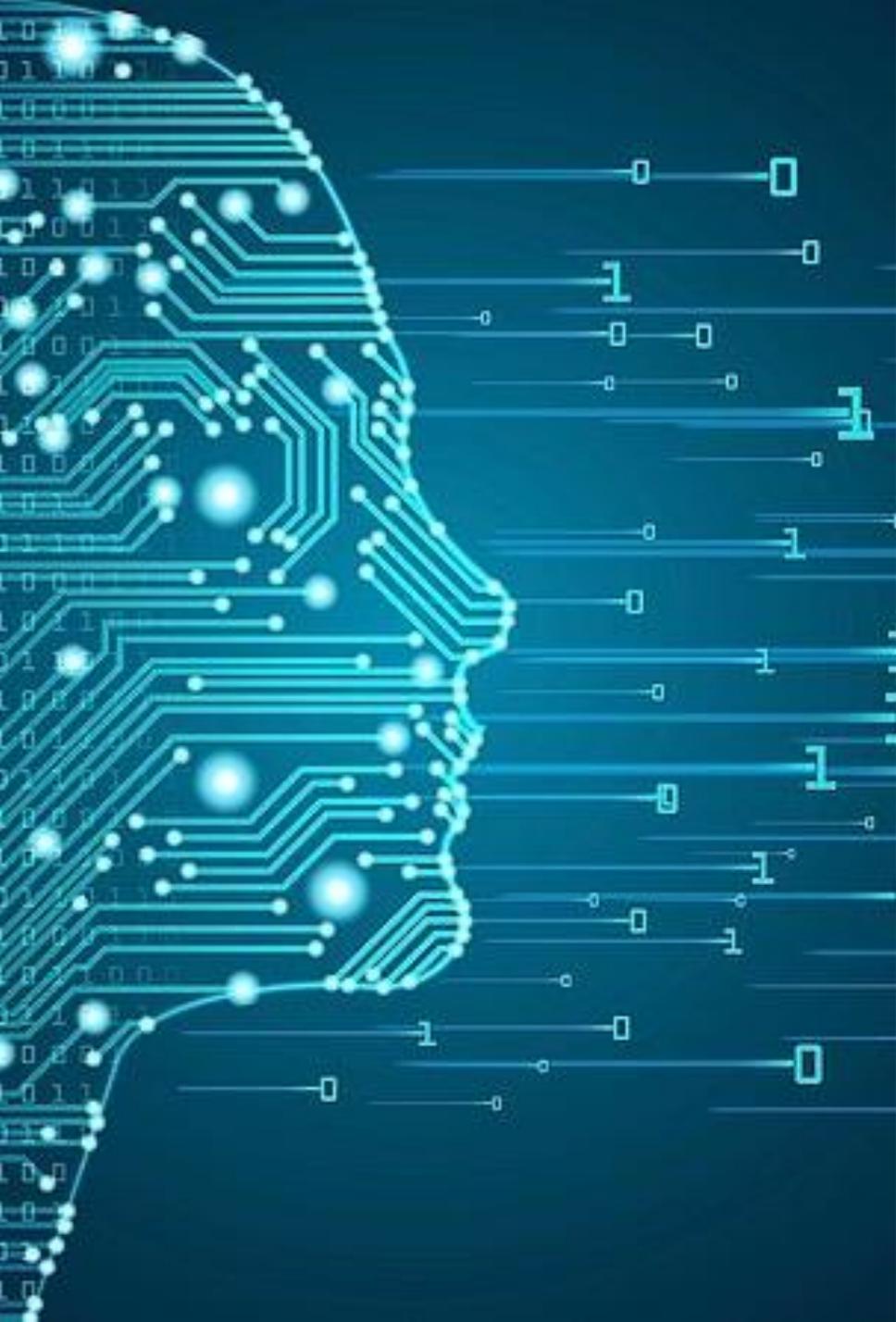
3. The AI regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities, **including at regional or local level (ITRE 72)**. Any significant risks to fundamental rights, **democracy and rule of law**, health and safety or the environment (AM 2313, 2314, 2316, 2317) identified during the development and testing of such AI (AM 2319) systems shall result in immediate and adequate (AM 176) mitigation.

Competent authorities shall have the power to temporarily or permanently suspend the development and testing process, or participation in the sandbox if no effective mitigation is possible (AM 2313) and inform the European Artificial Intelligence board of such decision without delay.

4. Participants in the AI regulatory sandbox shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result of (AM 177, 2321) the experimentation taking place in the sandbox. **However, provided that the participant(s) respect the sandbox plan and the terms and conditions for their participation and follow in good faith the guidance given by the authorities, no administrative enforcement action shall be taken by the authorities for infringement of applicable Union or Member State legislation (AM 2315)**

4a. Upon request of the provider or prospective provider of the AI system, the national competent authority shall provide, where applicable, **a written proof** of the activities successfully carried out in the sandbox.

5. National competent authorities shall make publicly available **annual reports** on the implementation of the AI regulatory sandboxes, including *good practices*, *lessons learnt* and *recommendations* on their setup and, where relevant, on the application of this Regulation and other Union legislation supervised within the sandbox

The modalities and the conditions for the establishment and operation of the AI regulatory sandboxes under this Regulation shall be adopted through **implementing acts**
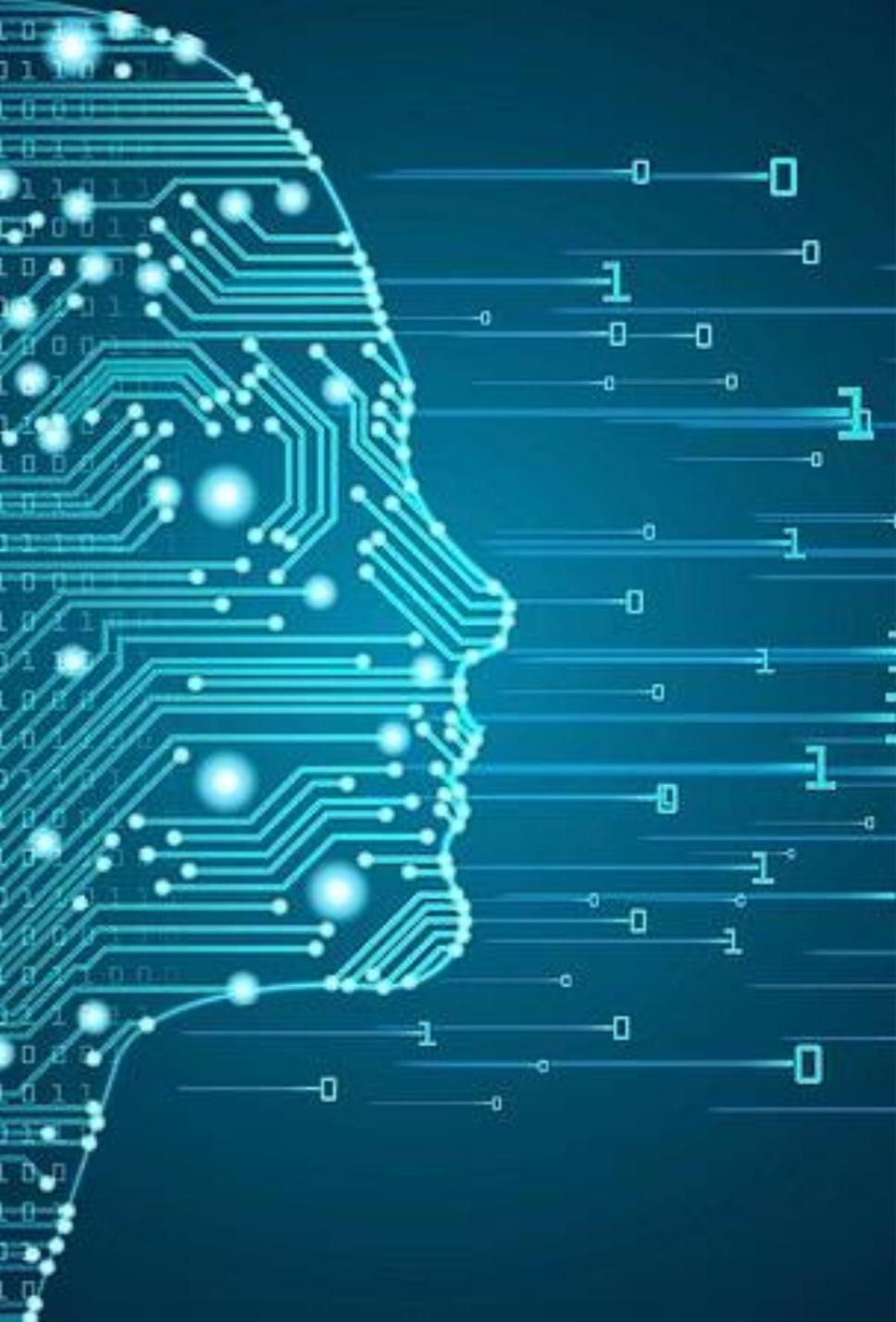
When national competent authorities consider authorising **testing in real world conditions** supervised within the framework of an AI regulatory sandbox
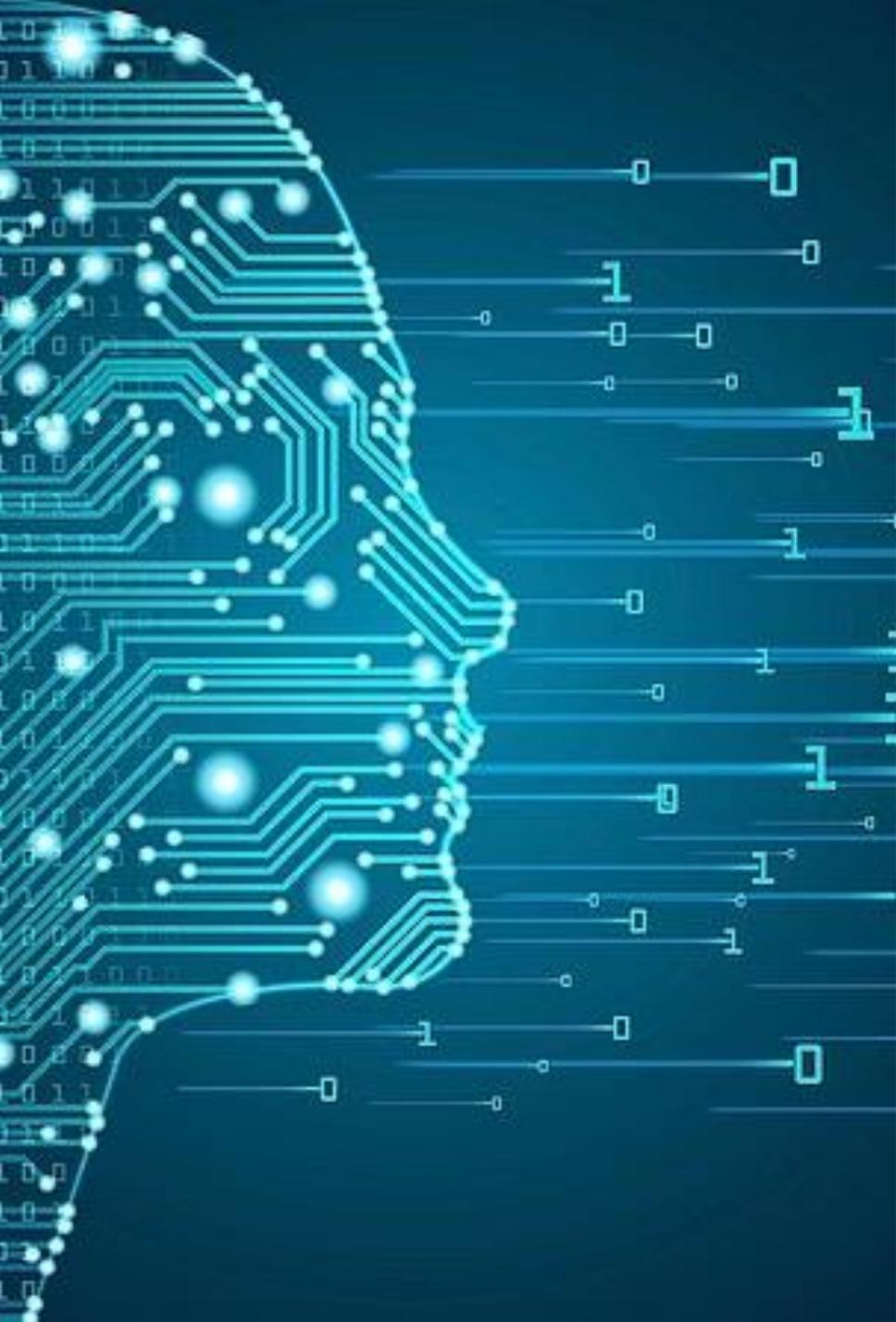
Article 54 Further processing of **personal data** for developing certain AI systems in the public interest in the AI regulatory sandbox
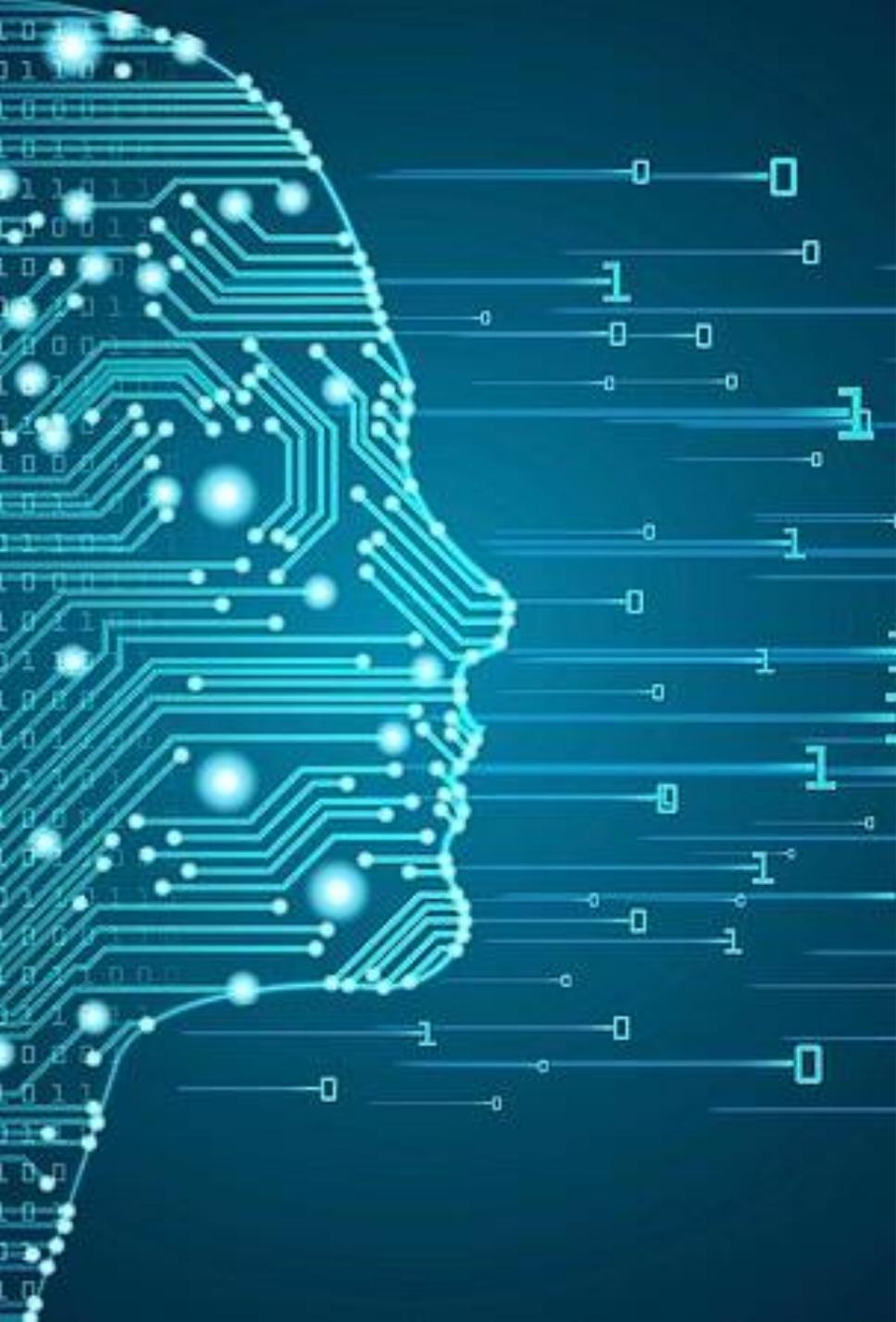
Art. 54 – continued:

In the AI regulatory sandbox personal data lawfully collected for other purposes may be processed for the purposes of **developing, testing and training** of innovative AI systems **in the sandbox** under the following cumulative conditions:

- AI systems shall be developed for safeguarding substantial public interest;
- the data processed are necessary for complying with one or more of the requirements to mitigate bias where this cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data
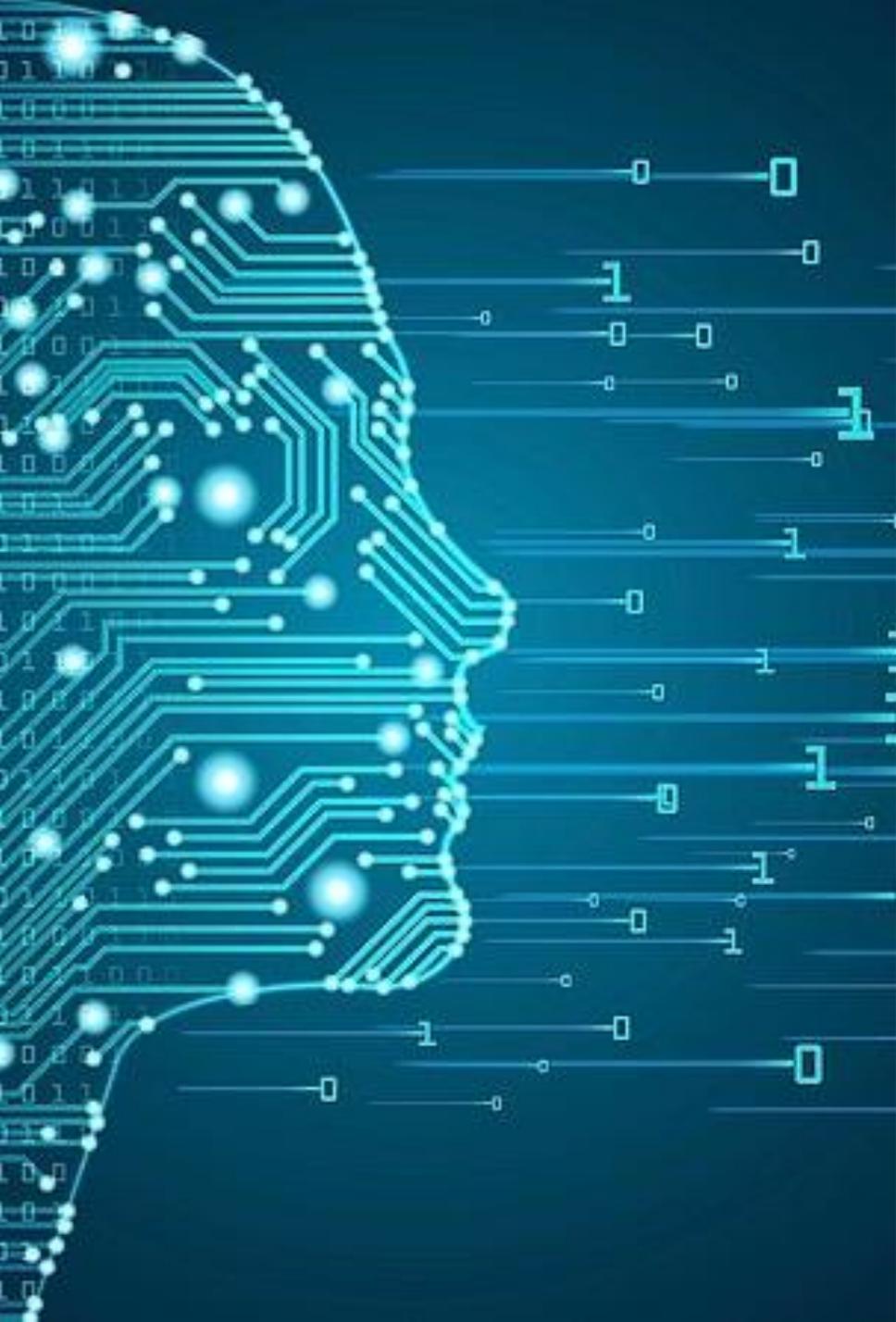
Article 54

Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox
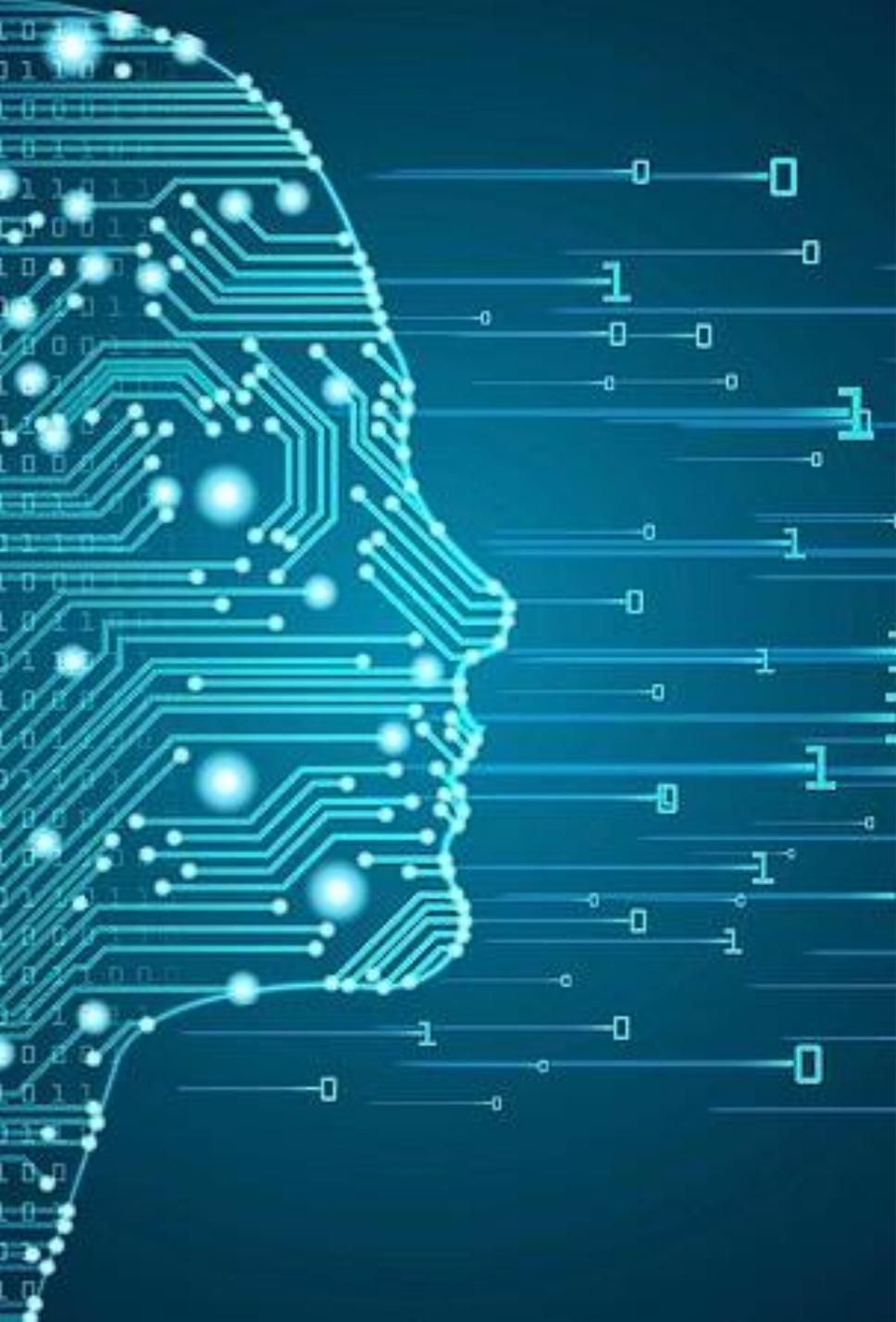
Article 10

Data and data governance

3.   Training datasets, and where applicable, validation and testing datasets, including the labels (1718), shall be relevant, representative, up-to-date, and to the best extent possible, taking into account the state of the art and in accordance with industry standards, (AMs 96; 1715; 1716; 1718; 1720; 1721) free of errors and be as complete as possible (AM 96). They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which in relation to whom (AM 1722) the high-risk AI system is intended to be used. These characteristics of the datasets may shall (AMs 1712; 1718; 1719) be met at the level of individual data sets or a combination thereof.

5.   To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued. (AM 98; 1734; 1735; 1736; 1737)
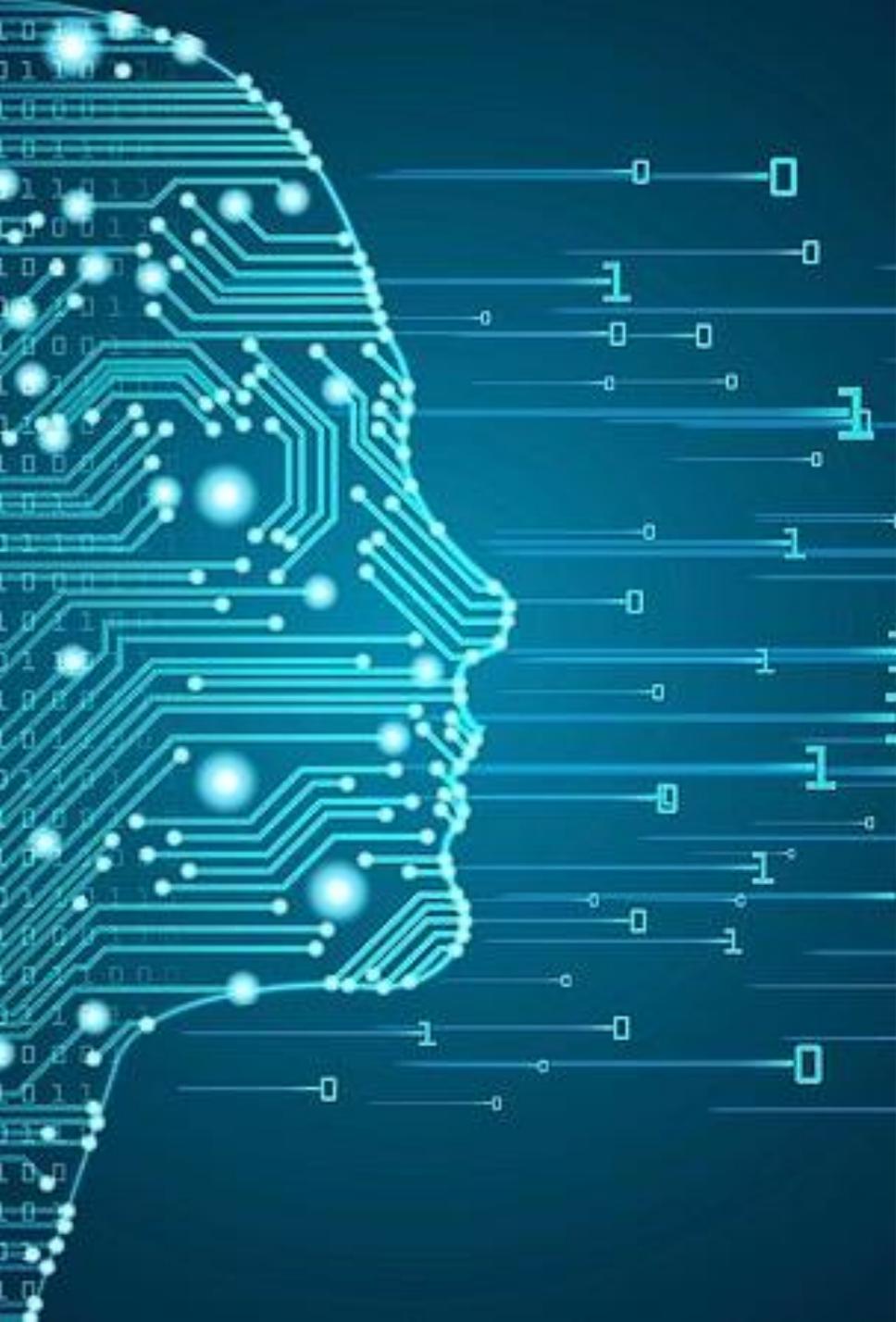
Article 54a Testing of high-risk AI systems in **real world conditions** <u>outside</u> AI regulatory sandboxes

Ursula von der Leyen: promote uptake AI and address risks

TWO PROPOSALS:
Product Liability Directive (PLD)
&
AI Liability Directive (AILD)

Timeline: the new regimes could be fully in force across Europe in 2024-25.
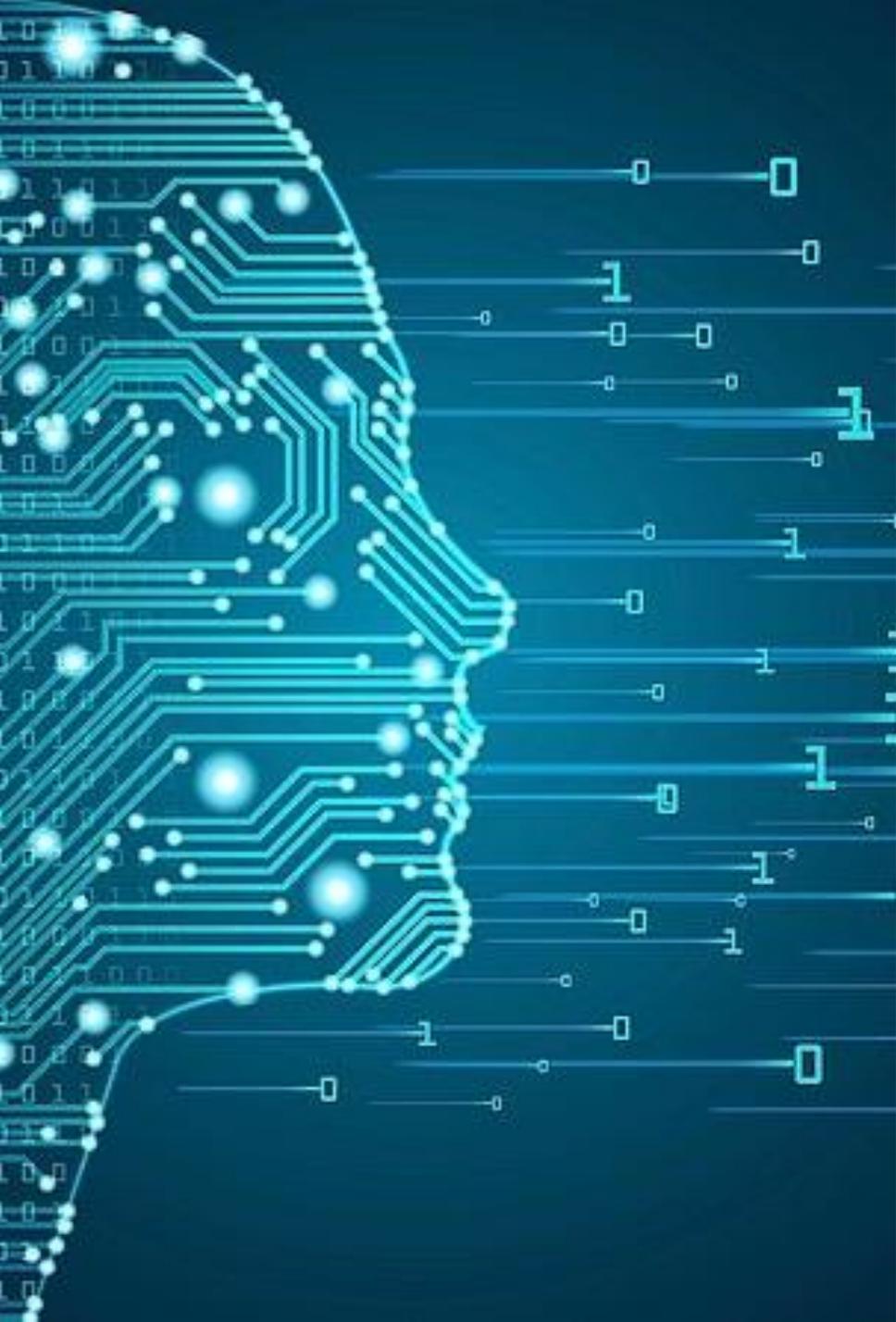
Interrelation PLD and AILD:

AI-enabled products and AI-systems would fall within the scope **both** of the new AI-specific regime and the revised Product Liability Directive

>AILD: `'fault based`'
>
>PLD: "strict liability".

Applying these different regimes in practice may be challenging both for courts and litigators.

AILD
Causality presumed re high-risk systems, if <u>provider</u> failed to comply with requirements of AI Act, regarding:

- Training data

- Transparancy

- Effective oversight

- Appropriate level of accuracy, robustness and cybersecurity

- Corrective actions

Secondly AILD
Causality presumed re high-risk systems, if
<u>user failed to </u>comply with requirements of
AI Act, regarding:

- Use or monitor in accordance with instructions

- Exposed to input data which is not relevant in view of intended purpose

QUESTIONS?