MACEDO VITORINO

ARTIFICIAL INTELLIGENCE

THE EU AI ACT OR HOW TO PUT AI IN A BOX

António de Macedo Vitorino

The European Union wants to be at the forefront of the regulation of artificial intelligence. The European Artificial Intelligence Act ("AI Act") aims to serve as the blueprint of future AI regulation in the world, in the same way as the General Data Protection Regulation ("GPDR") became the basis for regulation of data protection in many countries.

The advances in EU AI legislation are now seen as blocking investment in the field of AI with the risk of increasing Europe's lag in relation to the United States and China, and the exodus of its most talented engineers to locations free from the constraints of the AI Act.

The EU AI Act defines AI as "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".

The companies that will be most affected by the AI Act are the developers of AI systems placed in the EU or whose system's outputs are used in the EU as well deployers, importers and distributors of AI systems.

Annex I of the AI Act lists the techniques and approaches that are considered as AI which include among other things:

- Machine learning, including supervised, unsupervised and reinforcement learning, using a wide variety of methods, including deep learning;
- Logic and knowledge-based, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; and
- Statistical, Bayesian estimation, search and optimization methods.

The EU AI Act chooses not to define artificial intelligence as a form of intelligence or intelligent behaviour, but as a series of technical tools with advanced capabilities. This choice is deliberate and shows that AI cannot be defined, even by approximation, as human intelligence. Taking the words of the AI Act on their face value the various techniques and approaches could be interpreted as including any algorithm or even any computing machine (going as far back as to the first computing in the fifties of last century) which can hardly be considered "intelligent" and more importantly could pose serious issues in present economic activities.

Because of the wide scope of its definition of AI, the EU AI Act excludes some techniques which are not to be considered as AI for the intended legal purposes:

- Software that does not generate outputs influencing the environments they interact with;
- Software that is solely based on predefined and static rules; and
- Software that is solely based on random generators.

These exclusions serve to free many existing technologies from the burden of the new regulation. Does this approach work? Most likely not, as the cumbersome set of rules imposed by the AI Act demonstrate.

It is apparent from the AI Act that the European lawmakers are not trying to regulate AI but to limit the "scary" consequences of the wide adoption of many technical systems that can be used to invade privacy or menace the wellbeing of human societies in general.

The core of the EU AI Act is not AI but the risks of advanced technical systems, which working separately or in conjunction can severely create risk for democracy, privacy or liberty. Face recognition systems are a good example of a technical advance that is not analogous to human intelligence (as it also exists in animals) and yet has the potential for creating a dystopic society or used to threaten and coarse individuals.

The EU AI Act looks at the potential dangers to classify AI systems (all of those in Annex 1) into four levels:

- **Level 1**. Unacceptable risk systems that are prohibited, which includes systems considered as threatening people's safety, livelihoods and individual rights.
- **Level 2**. High risk systems, which are highly regulated, including systems that negatively affect safety or fundamental rights.
- **Level 3**. Limited risk systems, therefore requiring only certain transparency obligations, which include lower-risk AI systems, such as chatbots.
- **Level 4**. Minimal risk systems that call only for voluntary codes of conduct, such as spam filters and recommendation systems.

The application of this classification alone requires massive auditing work for businesses using and developing AI systems or software systems with AI components. Toll road managers, traffic controlling companies, banks, insurance companies, hospitals and health providers, courts and public authorities, among many others, will one way or another be affected by the application of the AI Act because they all use systems with AI components.

Many companies develop software tools using AI components, not only in the wide sense AI is defined by the AI Act but also including some of the "scary" elements of AI so much feared by EU legislators, such as face recognition or risk profiling based on background information that might ultimately lead to social, gender and racial biases even when such biases are not built-in from exiting biased data.

The AI Act is an attempt to put AI in a box that misses the real points of concern. It is not the technology that must be regulated but the wrong use of technology.

The following are the real points of concern that call for urgent regulation:

- **Mental conditioning and mental warfare systems**. Mental conditioning systems powered by AI are already in place. We see them every day in social networks, which use AI algorithms to promote engagement and favour the dissemination of fake news and promote aggressive behaviour. Leading people to illegal and vicious content in a conscious and deliberate manner should be prohibited and punished;

- **Use of personal data**. The data used in the models is not open for anyone to use. Consumers that publish posts, reels, photographs, video, text etc did not sign up for unrestricted use of their data by machines to do whatever the owners of those machines wants. Personal data should not be used for training, pattern recognition, marketing or similar activities.

- **Use of proprietary data**. Authors, publishers and media companies are raided everyday by AI systems. Their data is used to train models and to create new data. No consent was given to AI systems' owners to use such data. Usage by AI systems does not fall under the "private use" rule anymore. Copyright owners should have full control of any use that is not made by a human being.

Unfortunately, failing to correct what is wrong is not the only problem with the European regulatory spree. Another consequence of the AI Act is to scare off local and international investors, European entrepreneurs, start-ups and software developers.

If Europe does not backtrack some of its existing policies and does not create a favourable legal, economic, tax and regulatory environment, it will lose the AI war that is looming and be for a long time at the mercy of the United States and China and others that may come along.

CONTACTS

António de Macedo Vitorino

Email: avitorino@macedovitorino.com

Telephone: 351 213 241 911