NORA Norwegian Artificial Intelligence Research Consortium

June 10, 2021

Comments to "The Artificial Intelligence Act"

Thank you for giving NORA the opportunity to comment the proposed regulation and give input to Norway's national position on the European commission's proposal for a regulation on artificial intelligence, The Artificial Intelligence Act.

NORA is a national consortium for research, education and innovation within the fields of artificial intelligence, machine learning and robotics. The consortium has 12 partners; eight universities, two university colleges and two research institutes: University of Oslo, University of Bergen, University of Stavanger, UiT The Arctic University of Norway, OsloMet, University of Agder, Norwegian University of Life Sciences, NORCE, Simula Research Laboratory, Østfold University College, Kristiania University College and University of South-Eastern Norway.

The expertise within the NORA consortium covers all aspects of AI.

General considerations

It is highly challenging to have a technical regulation of emerging technologies. Any too technical defined regulation may quickly render itself obsolete or even counterproductive. This dilemma is a well-known double-bind problem, often referred to as at Collingridge dilemma. Impacts of technology cannot easily be predicted or regulated in detail before we know how the technology unfolds. However, when technology is already unfolded, it may already be too late to regulate. As such, it is a good approach to regulate based on the intended purpose of the AI systems, not the technology or algorithms in itself. This has the potential of making the regulation future-proof.

The current regulation more or less follows a precautionary approach, meaning that it is up to the implementers to show that it works as expected by, e.g., claiming accuracy and fairness. Hence, the regulation needs to be broad. However, there are several topics in the suggested regulations that are too vague.

The regulation would benefit from a stronger connection to existing laws and regulations, such as the General Data Protection Regulation (GDPR). There is a certain overlap, e.g., logging of high-risk systems and traceability of results are linked to right to an explanation.

The impact of the regulation on the competition between the big tech giants and SMEs should also be commented upon. It has been harder for SMEs than for the bigger companies to adapt to General Data Protection Regulation (GDPR). We believe the suggested regulation has the potential to even out the playing field for big tech giants and SMEs. Although the big tech giants have adapted to GDPR, we have seen several times that big tech giants often claim high level of accuracy in their AI systems without backing it up with evidence. IBM is an often-used example, where Watson health has overpromised and, in many cases, failed quite miserably. SMEs, on the other hand, would traditionally have to prove their system to a much larger extent. It is important to level the playing field in order to promote competition.

NORA

Below we comment certain points we find relevant, illustrating these general considerations.

Specific comments

- **GDPR:** The relationship between GDPR and The Artificial Intelligence Act needs clarification; see the submitted input from SERI, University of Oslo.
- **Definition of risk:** The differentiation between risk levels, e.g. high-risk and limited-risk, is often vague; for example, biometric analytics and mass surveillance. When is a place considered public? Is an app public? These details need to be panned out.
- **Discrimination by interaction:** Note that although an AI algorithm is developed so that it does not discriminate individual groups it could still discriminate if we combine groups. For example, an algorithm that do not discriminate women or black people could still discriminate "black woman". Such discrimination by interactions of terms may be very problematic and hard to disclose. Thus, the regulation should not only focus on groups, but discrimination in general, including discrimination by interactions.
- **Surveillance and AI:** Poorly designed systems could enable unwanted surveillance. The solution is to build these considerations into the system itself, rather then rely on policies alone.
- **Privacy by design**: A badly designed AI system is a danger for privacy. The regulations should promote privacy by design.
- **Explainability**: The regulation should define what an explanation of AI is. What constitutes an explanation of the black box of AI?

We hope these points will be taken into consideration. Don't hesitate to contact us for further contributions to the process.

Yours sincerely,

Klas Pettersen

CEO, NORA