Artificial intelligence association of Lithuania position on EU AI Whitepaper

We would like to express the support for the AI whitepaper initiative of EC. Private sector supports the initiative to ensure the policy does not increase fragmentation within the EU, this is of utmost importance in order to be competitive in the global economy.

Main points we do and do not support

Positive aspects:

- Encourage development and promotion of AI, as well as breakthroughs AI technology
- Promote creation of reliable and sophisticated products
- Foster transparent, awareness-based and risk-cost-benefit based models for assessment, evaluation and, eventually, regulation of AI
- No fragmentation policy within EU
- Support uniform horizontal approach to all core aspects of AI within EU
- Create AI excellence centers
- To create the Digital Innovation Hub and ensure access to AI for SMEs

Negative aspects:

- The regulations based on technology and application:
    - EC should recognise and separate three moving and interacting particles: AI technology *per se*, final application domain and potential risk of application.
    - The high-risk domain specific application products might have explicit regulations.
    - Currently most of the different domains already have regulations in place, which cover the usage, consumer rights, health regulation, product liability and lay down respective requirements.
    - Broad regulation may introduce inadequate regulation in no or low risk applications or introduce regulation misinterpreted by local authorities causing development and application restrictions.
- Human in the loop requirement (confirmation, second opinion)
    - Certain areas where insisting on a human person to be in the loop may decrease overall performance of the AI based system both speed and quality-wise.
        - Example: where an AI has demonstrated to be more accurate than a radiologist at making diagnosis, allowing a human doctor to overrule would risk a less accurate diagnosis;
        - Example: The airport security systems that are already in place would require some partial deautomation, and also introduce additional human error.

    - High-risk definition
        - We have to make sure that AI regulation is not rushed since it is addressing effectively the key concerns of citizens as well as the private sector. Currently the definition of AI is too wide and high-risk applications are basically include all EU industries;
        - EC already has the AI testing facilities initiative which will cover the testing of AI products
        - The definitions should not focus only on the risk, but should take into account the probability of this risk happening. Regulators should think also about potential economical and cost of not integrating AI into certain areas for example: health sector;
- Data validation
    - Hard to imagine a regulatory specialist that would be able to assess the data validity or quality for a specific task. The approach where someone provides detailed information about his data and shows that on his data AI is bias free does not prove it is bias free. Also all reproducibility of AI products during life-cycle would require collecting all the user data during product use which is contradiction with GDPR and possibly violating human rights and European values.
    - The neural network training process is highly susceptible to training parameter tuning, data content distribution, order of training substages, versions of software used that controlling or loging them in a standardized way is virtually impossible.
    - It's important to mention that personal data use and management is already covered by GDPR.
    - The free flow of non-personal data is accordingly covered by EU Regulation on the free flow of non-personal data
- Liability and AI
    - Initiatives for reviewing the legal liability regulation for AI firstly should be based on assessing existing regulatory frameworks and identifying problematic areas.
    - New overlapping regulations are likely to discourage AI development and research in the EU.
- Ex-ante
    - Ex-ante regulation will likely have negative effects on Europe applying AI in its key sectors. For the most research areas of where AI may be applied, it's difficult and often impossible to predict the AI model performance before it's developed and tested;
    - Proper self regulatory processes should comply with EU principles.

Good practices of ‘black-box’ testing and AI usage in high-risk domains

Usually when we talk about AI based products only a small number of components of the product actually use AI. That same AI is usually integrated as a ‘black-box’ technology. We would like to draw attention to multiple good practices which have proved themselves in testing AI technology and also explain how these practices could be successfully applied within the EU. An example we’d like to expand upon is biometric recognition. Most of the biometric recognition algorithms nowadays are based on modern AI technologies. Nevertheless these AI based biometric technologies are widely used in highest-risk applications: airport checking systems, voting registration, law enforcement tools. The reason why these high risk scenarios employ AI is trust. Trust comes from clear and transparent technology testing methodologies and procedures that are used to test various algorithms regardless of being AI based or classical. The most widely recognized organisation that performs these tests is the National Institute of Standards and Technologies of the USA (NIST). NIST provides public reports on testing algorithms in near real conditions, and provides a basis for using even ‘black-box’ models in highest-risk domains. These reports are referenced to formulate requirements for various risk level systems. EC already has a plan to create AI testing facilities, so these facilities could be used to test and evaluate various kinds of AI technologies including ‘black-box’ AI technologies in a similar way.

The EU wide organization (NIST analogy) could do all kinds of AI evaluation from multiple perspectives like rase, age bias and produce public reports (e.g. NIST face matching evaluation FRVT 2009, includes age, race, sex biases and other quality and speed parameters). These reports would show (as it does at least for fingerprint, face evaluations in NIST) the ranking against the competitors which in turn stimulates competition among AI researchers. Then evaluating the risk of the final system would be dependent on a specific application scenario. Such approach allows to separate application evaluation from AI research and development - protecting research and development from overregulation. At the same time providing a framework for quality assessment and improvement. This approach would place the burden onto AI integrators of finding the right AI algorithm or proving to governmental institutions that the solution is safe. Application specific regulations could allow defining quality or bias thresholds that would then be compared against reported AI performance. Also such reports would make it easier to choose the right AI solution, and would make a level playing field for AI research and development.

EC Whitepaper underlines that the EU has to become the world leader in the AI field. Thus we need to ensure that research and development of AI is encouraged within academia as well as within the private sector. However we also acknowledge the necessity to ensure the safety of AI products that will be used by the general public. Having said that, it is important to remember that almost all underlining AI technologies are independent of application scenarios. For instance a human voice synthesizing AI technology can be used either for preserving a voice of

a loved one or to be used to spread misinformation by pretending to be a reputable public person. It is also crucial to understand separation between AI research and development from real world applications. We should encourage the development of the technology in general, but when the company is providing the end product it must ensure the product behaves as promised.
There are many biometric companies from the EU that are among the leaders in the world: French companies Thales, Idemia, (ex Morpho, Sagem), Innovatrix from Czech Republic, Neurotechnology from Lithuania, BioID and Dermalog from Germany just to name a few. Biometrics falling under high-risk classification means strict regulations which are likely to diminish the advantage of EU biometric companies on the global stage.

AI vs Human quality scale

To protect from people unreasonably choosing an algorithm that is better by a miniscule amount comparing 1st and 10th place algorithms, one could rate the algorithm in times it performs better than the human. It also would remind people that if there is a mistake a human would perform worse, and maybe mistake is not part of AI but rather the part of the system that is not AI.
Alternatively the AI rating instead of indicating times AI is better than human performance but there could be grades, e.g. letters F-A, where letter would represent performance on a log scale. C for instance would mean AI makes 10 to 99 times less mistakes than a human, b 100-999 times less mistakes, A more than 1000 times less mistakes. The actual rates can be chosen by analyzing current state of art and harmonizing between different AI applications. Or having letters represent different rates depending on the problem (face recognition, navigation…), on the other hand differentiating between fields may add unnecessary complexity.

Remote biometric identification

Remote biometric identification definition is ambiguous. In academia *remote identification at a distance* is used in the sense that is used in the whitepaper. Remote identification can be confused with a biometric processing server in a distributed computation system where single or operators dealing with biometric data can work at remote locations and biometric data processing is performed at centralized server (cloud computation solutions). Such a scheme is common for large scale systems: airports, voting registration, law enforcement tools. Also there are touch-less fingerprint scanners, with current terminology use one can assume they should be considered as remote identification. Same can be said about handheld iris-cameras, vein scanners? Definition should rather include active/purposeful voluntary participation from a subject in the identification process.

Conclusions

Overall we support the necessity of limited umbrella AI regulation to ensure no fragmentation policy within the EU. However, we stress that the current document needs significant rethinking and should be improved. We explicitly define various risks as well as economical impact if the

whitepaper version would be as it is. More important, we suggest good practices, and suggestions on how to improve critical points of whitepaper.