IMPACT AI

Impact AI Position Statement on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

05 AUGUST 2021

Created in 2018, the French think tank Impact AI aims to explore ethical and social issues linked to artificial intelligence, as well as to build a better world through the support of sustainable initiatives. With more than 60 listed members, large enterprises, SMEs, consulting firms, start-ups, universities and NGOs, Impact AI makes its vocation to work with the entire digital ecosystem. The think tank associates economic players, institutions, research organisms and societal stakeholders to its actions, in order to create a responsible and inclusive approach of AI.

More about us: www.impact-ai.fr

Dear Sir/Madam,

Impact AI welcomes the European initiative to establish first ever legal framework on Artificial Intelligence (AI) aiming to promote Europe's innovation capacity in AI while supporting the development and uptake of ethical and trustworthy AI across the European Union (EU). It is a great achievement and a worldwide leading initiative that opens the path to an appropriate use of the leading-edge AI technologies in the world.

While AI has become a clear and undeniable force for business disruption and transformation, it also entails certain risks, such as potentially exposing people, including children, to significant mistakes that may undermine fundamental rights and safety, gender-based or other kinds of discrimination, opaque decision-making, or intrusion in our private lives.

Faced with the rapid technological development of AI and a global policy context where more and more countries are investing heavily in AI, the European Commission (EC) has acted and proposed a project for regulating AI usage.

At Impact AI we believe that designing and implementing frameworks to manage AI usage in an ethical, robust, controlled and secured manner is key for supporting adoption and holistic transformation of the organization. We have created a task force and communicated on the market on the best practices to deploy trustworthy AI across organizations.

We believe that this kind of legal regulation is necessary to guarantee the fundamental rights of EU citizens and residents. However, the Proposal of the EC is rather risk-oriented neglecting the wonderful benefits and opportunities the AI can bring to European citizens, to the society as well as to both the European economy and the economies of our trading partners.

As a group of companies representing several industries and of different sizes, we wanted to take the opportunity to share some comments on the core principles and themes that we consider important when promoting the uptake of trustworthy AI in Europe.

We thank you in advance for your consideration.

Best regard

TABLE OF CONTENTS

1. Governance

a. Conformity assessment

- More details are required on the way the conformity assessment should be carried out as this is a time consuming and expensive procedure.

- The EC should further specify the nature of conformity assessment in different scenarios:
    - Should conformity assessments be carried out on a voluntary basis or by a third party?

- Clarification is necessary regarding the introduction of certifications:
    - What can be certified?
    - Who can certify?
    - What type of certifications can be used?

b. European Data Protection Supervisor (EDPS)

- European Data Protection Supervisor (EDPS) is designated as the competent authority and the market surveillance authority for the supervision of the Union institutions, agencies, and bodies when they fall within the scope of this Proposal. However, the role and tasks of the EDPS are not sufficiently detailed and should be further clarified in the Proposal, specifically when it comes to its role as market surveillance authority.

c. European AI Board (EAIB)

- The composition of the AI Board and the role of company experts (if possible) should be specified more precisely. The Proposal foresees to give a predominant role to the EC in the EAIB. Not only would the latter be part of the EAIB, but it would also chair it and have a right of veto for the adoption of the EAIB rules of procedure. This contrasts with the need for an AI European body independent from any political influence. Therefore, we believe that the future AI Regulation should give more autonomy to the EAIB and ensure it can act on its own initiative, in order to allow it to truly ensure the consistent application of the regulation across the single market.

- This entity should have the vocation to help AI system development and deployment, rather than stifling innovation.
    - How exactly the AI Board will be organized and how it will operate?
    - How the experts will be nominated?
    - How much those independent experts will be involved in the development of the EU policy on AI?
    - What will the mandate of this entity be?

d. The role of industry experts and national institutions

- Industry experts should take an important part in the establishment of this framework, as they are the ones who will be applying the AI Act in real life. This would render the framework more practical and operational.

- How the EC intends to incorporate AI practitioners' opinions and contributions to the regulation of AI?
- Will there be an institution or a board where representatives from different industries and academia could directly share their position on AI regulation in the EU?

- The role of national institutions should be specified in a more detailed way.

2. Industrial impact

a. Flexibility of the AI Act

Benefits

- The AI Act focuses on the deployment of AI systems based on their risk-level regardless of the industry they are implemented in. This flexibility of the legal framework is very important to accommodate future technological developments and dynamically adapt as new concerning situations or solutions will emerge.

Risks / Inquiries

- The EU AI Act is rather risk-oriented and does not account for cases where AI is actually beneficial for the society and the economy. We believe that this perspective is not satisfactory as AI risks and benefits are of the same nature[1]. Hence, a thorough analysis of AI benefits / risk ratio, as well as individual / societal impact[2] of AI should be conducted. This way, the risk level of AI systems would be appreciated more appropriately.

- Some very important industries, such as health, pharmaceutics, autonomous cars, are not developed in the regulation while they may be subject to high risk AI usage with direct impact on human health, safety, and security.
  - Why those topics are not included in the AI Act?
  - Is this a very specific matter that will be covered by other (maybe upcoming) regulations?

- AI technologies can help support Europe in achieving its green deal objectives. However, AI itself has a significant environmental footprint, especially in terms of energy consumption.
  - EC may also consider providing guidance on key performance indicators to identify and measure the positive and negative environmental impact of AI.
  - The Environment being one of the most important assets, should it be treated as a separate entity with special protection requirements?

- Further clarifications are required regarding 'real-time' and 'post' remote biometric identification systems:

[1] For example, AI can be used to increase the security of the society, but AI can at the same time undermine that security.

[2] AI systems bringing grate opportunities for the society as a whole may be rejected because of their potential impact on an individual level.

- What will be the procedure for getting a prior authorization for 'real-time' remote biometric identification system in publicly accessible spaces?
- What will be the procedure for getting a prior authorization during or after the use of 'real-time' remote biometric identification in a duly justified situation of emergency?
- To be categorized as 'post' system the remote biometric identification should occur only after a significant delay. Would it be possible to add clarifications on what should be understood as "a significant delay" as well as the requirements on the material involved?

- More details should be provided regarding the transitional / adjustment period granted to companies to get compliant after each yearly revision of high-risk AI system characteristics by the EC.

- Some of the terms mentioned in the Proposal, such as "essential private services", "high quality data", "explainable AI systems" should be clarified.
  - For example, is the justification of the AI system's behaviour by an expert enough to consider it as explainable? Should the context be taken into account? Should the explanation take place in real time?
  - This ambiguity of certain requirements will certainly produce a proliferation of norms. However, the promulgation of those standards will take some time. Hence some common guidelines should be established to help AI system provider's while those norms are being established.

b. Impact on business activities, innovation, and competitiveness

Benefits

- The establishment of effective and harmonized rules could improve business activities by fostering the development, use and uptake of trustworthy AI in the EU.

- The proportionality of the EU framework imposes regulatory burdens only when an AI system is likely to pose significant risks to fundamental rights, health, and safety. Hence, the deployment of most real-life use cases will not be restricted at all as they do not present a risk for individuals.

- The commonly established norms and standards will not only promote trustworthy AI that is consistent with Union values and interests, but also will create a best practice repository and benchmarks that companies will have to line up with. This standardization of code of conduct and jobs will increase transparency and traceability, facilitate the control of business activities and AI system comparisons.

Risks / Inquiries

- The EU encourages national competent authorities to set up regulatory sandboxes. The absence of common guidelines for all EU Member states may increase the gap in terms of innovation opportunities, algorithm testing and improvement, and competitiveness. We

believe this may have a negative impact on the effectiveness the AI Act in achieving the goals established by the EC.
More details should be provided on the way AI regulatory sandboxes will be used to develop AI systems in the public interest.

- Which entity will be charged to provide this controlled environment?
- What type of controlled environment is it (infrastructure, central repository…)?
- How long these sandboxes will be available for?
- What will be the framework and the rules (security, policies, encryption…) to support the sandboxes?
- These controlled environments are available before the placement on the market or putting into service of AI systems pursuant to a specific plan. Who will be in charge of assessing and prioritizing those plans?
- Will it be possible for companies to use those regulatory sandboxes to test and improve their high-risk AI systems (for example with fake data) without immediately engaging to any conformity assessment requirements? Those requirements will be satisfied only for AI systems that will be selected after sandbox test. This approach may encourage industries to innovate, and to create new products.
- What would be the solutions/tools/guidelines provided and/or expected on the sandboxes to support the assessment and confirmation of the respect of trustworthy and ethical AI principles?

- The failure to formulate effective regulations will slow down investment and dampen the development of the European market compared to leaders in AI such as the USA or China. European entities that are directly affected by this regulation will have more restrictions to follow and requirement to satisfy than non-European entities leaving them in a less favorable position regarding algorithm testing and improvement.

- Some already heavily regulated sectors are targeted by the AI Act. How will the EC ensure that those restrictions will not be cumulative in order to avoid over-regulation or contradictory statements which may have a negative impact on company's competitiveness?

c. Source code protection and algorithm sharing

Benefits

- The EU database could improve the confidence in AI systems by increasing transparency, traceability, oversight and strengthen ex post supervision by competent authorities.

- In health, the European health data space will facilitate non-discriminatory access to health data and the training of AI algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance.

Risks and challenges

- An exactly and sharply stated definition of source code should be provided:
  - How can the source code be qualified?

- Is data included in the source code?
- Are libraries, machine codes or other elements included in the source code?

- The treatment and export of "classified" models[3] should be considered in detail in the regulation.

- More information is required on the possibility to apply reverse engineering:
  - How and when should it be applied?
  - Should there be an application and usage distinction by industry?
  - Will it be possible to elaborate the legal basis for reverse engineering, such as definition of the NDA scope?
  - What guarantees could be provided to avoid losing secrets and patents due to reverse engineering when conducted with malicious intent?

- More details should be provided on the how source codes will be rendered available for the EC:
  - Will they get an access to the company's infrastructure or the code will be handed on a specific device?

- Code analysis is another aspect that should be further developed:
  - Will the code itself be analyzed (line by line approach) or only the results produced by that code (more pragmatic approach)?

- Intellectual Property Leaks: Caring about the overall security of the source code is vital to the health of any organization, regardless of its type, its size, and any other characteristics. Source code can be likened to the 'secret sauce' of a company. The code represents the intellectual property at a fundamental level – it is the instructions that make software products work. It is also part of the competitive edge and is a highly strategic aspect of any company's innovation and place in the industry. The consequences of source code exposure include everything from allowing competitors to have an advantage to loss of innovative edge, financial costs, as well as creating security issues for the firm and customers.
  - How will the EC treat source codes after their registration in the EU database?
  - How and what type of privacy and Intellectual Property protection guarantees will be provided by the EC?

3. Methodologies

a. Lack of implementation guidelines

- The EC should establish more specific and common rules for impartial and unbiased AI system classification. Companies affected by the AI Act should dispose of precise guidelines to assess the impact of their AI systems on individuals and the society, as well as the probability of occurrence of that impact.

[3] "Classified" models refer to models that are trained using classified data such as personal sensible data, confidential data, or data on financial transactions.

- Principals to compare different AI systems should also be introduced.

- Whether they are end-users, simply data subjects or other persons concerned by the AI system, the absence of any reference in the text to the individual affected by the AI system appears as a blind spot in the Proposal. Indeed, the rights and remedies available to individuals subject to AI systems should be explicitly addressed in the Proposal.

- The lack of stringent implementation guidelines may also result in different national strategies of the AI Act application. As with the GDPR, some countries rigorously followed the rules established, while others adopted a softer approach.

b. No precise technical solutions to achieve compliance

- Some safety measures should be provided to verify the conduct of conformity assessment.
    - Who will oversee conformity assessments (national institutions, new entity)?
    - A more explicit definition of fairness and ethics is required.
      What would be the reference to guide fair and ethical use principles that may qualify AI usage as prohibited? As an example, would the exact location (demographic information) of an individual be considered as a non-compliance if used in a credit score?
    - How algorithm performance and data quality will be evaluated?
      For example, a precise definition for bias should be provided.

4. Conclusion

Even though Impact AI welcomes the Proposal of the Commission and consider that such a regulation is necessary to guarantee the fundamental rights of EU citizens and residents, we believe that the Proposal needs to be adapted on several issues, to ensure its applicability and efficiency.

Given the complexity of the Proposal as well as the issues it aims to tackle, a lot of work remains to be done until a well-functioning legal framework, efficiently supplementing the GDPR in protecting basic human rights while fostering innovation, can be established. However, some actions should be taken to reduce or eliminate the administrative and legal burden, that may be one of the main obstacles on the way to apply the AI Act.

In Impact AI we look forward to continuing our thinking and advocacy related to the EU AI Act going forward with more representatives from academia and affected communities.

Impact AI

39, Quai du Président Roosevelt

92130 Issy-les Moulineaux

www.impact-ai.fr

contact@impact-ai.fr