Commissariat à l'énergie atomique et aux énergies alternatives
Atomic Energy and Alternative Energies Commission (CEA)

Artificial intelligence – ethical and legal requirements
CEA Feedback on the roadmap / inception impact assessment

Feedback period: 23 July 2020 - 10 September 2020

Date of issue: September 8th 2020

CEA welcomes the opportunity to provide feedback on the Commission's Inception Impact Assessment for a European legal act aimed at addressing the ethical and legal issues raised by AI. We welcome the initiative objectives, in particular the intention to create a harmonised framework in order to reduce burdensome compliance costs derived from legal fragmentation.

It is worth noting, a trustworthy AI as explained in HLEG on AI is at the same time a lawful, an ethical, and a robust AI. It takes into account all the concerns reflected in the trustworthy AI assessment list such as technical robustness, safety, security, privacy, traceability, explainability, auditability, in addition to diversity, non-discrimination, fairness, and respectability of fundamental rights. Actually, there is no need for an entirely new legislation, as current European legislation and standards already address many of these concerns. However, they may have some gaps that need to be filled.

Below are our comments on the outlined legislative options.

- Option 1 - non-legislative approach to facilitate and spur industry-led intervention:
  option 1 is probably convenient for low-risk AI solutions. However, there is a need of a minimum legislation that classifies the solutions according to their level of risk. Self-reporting of compliance with the HLEG ethical guidelines must remain verifiable and auditable by law. The Commission's support and encouragement of industry-led intervention towards trustworthy AI is very important, however in no case can this replace the enforcement of legislations that define the responsibilities and obligations of AI solution stakeholders.

- Option 2 - legislative instrument setting up a voluntary labelling scheme:
  the diversity and multiplicity of uses of AI applications may make it very hard to have a simple labelling for applications with variable risks. On the other hand, a multitude of labelling depending on the use cases could be difficult to understand by the consumer. Particular attention should be paid to the concept of labelling that may lead to dangerous issues: labelling must always be carried out against a charter verifiable by a third party. Self-labelling involves too much risk with regard to its verification. CEA is not in favour of this option.

- Option 3a: legislation for a specific category of AI applications only, notably remote biometric identification systems:
  biometric identification systems must be subject to strong legislation. However, CEA considers it is more efficient to put in place a legislative instrument that applies to all AI applications and that modulates according to the AI application risk aspects.

- Option 3b: legislation establishing mandatory requirements for "high-risk" AI applications.
  "High-risk" AI applications should not be binary; there must be a gradation of risks as in all sectors with a safety or security aspect. Different rules adapted to the application risk levels (like those in the IEC 61508 standard) are needed.

- Option 3c: the EU legislative act could cover all AI applications.
  CEA supports option 3C. Laws and standards cover all human activity, but this does not prevent creativity, innovation and freedom of expression. On the contrary, the absence of laws and therefore an increase of incidents combined with a legal vacuum may impede the AI development and deployment.

In summary, CEA supports option 3C; however, legislation should consider an AI application like any software application. We cannot blame the AI: following the use case, the application providers, issuers, operators, or users are responsible for a malfunctioning of the applications.

Finally, changes in the system may regularly occur, thus the requirements of trustworthiness will be too light without a continuous risk assessment. There is a real need for more R&D in the risk area in order to conceive and create continuous risk assessment processes.