HealthManagement
Promoting Management and Leadership

Shaping the Artificial Intelligence of the Future

Prof Florencio Travieso, PhD
******@***em-lyon.com

Co-director of the MSc in Health Management & Data Intelligence, Law Professor - emlyon business school, France

In 2014, Stephen Hawking had warned that ‘the development of full artificial intelligence could spell the end of the human race’. [1] A bold statement indeed, but if we focus on the term ‘full’, we’ll understand that if not designed properly, certain level of autonomy that could be difficult to control and can be extremely damaging to fundamental rights.

Last April 2021, the European Commission unveiled the new artificial intelligence regulatory framework (AIRF), that will legally shape the way all actors in the sector integrate artificial intelligence in their activities. The main priorities are set on safety and fundamental rights of people and businesses, while increasing AI implementation, investment, and innovation.

Margrethe Vestager (Executive VP for Europe for Digital age and a recurring character in this column), warned us by saying that we should not fear AI, but build a technology that is trusted, safe and proactive for all of us.[2]

AI is known to be complex, opaque, unpredictable, autonomous, and a black box, constantly on the verge of becoming a HAL9000.

The AIRF opted for a general definition, as objective as possible (inspired in OECD principles), based mainly on the notion of ‘software’ developed using techniques ‘for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environment that interacts with’ (art. 3).[3]

This future regulation will pave the way for responsible AI that will allow the technology to become seamless, trustworthy and most of all, known. One of the key elements is education of users. This means to make information on AI available for all.

Risk is the Measure

The proposed regulation is considering the need to regulate in relation to the level of exposition to risk. Instead of wholly legislating on all AI-derived actions, the regulation is risk-driven. The regulation has created three categories: Unacceptable-risk, High-risk and Limited-and-minimal-risk.[4]

‘Unacceptable’ includes subliminal, manipulative, or exploitative and harming systems; real-time remote biometric systems used on public spaces and social scoring based on evaluation of trustworthiness social based on social interactions.

‘High-risk’ includes systems that perform credit rating analysis on users, recruitment tools, employee management and biometric identification.

‘Limited-and-minimal-risk’ includes systems with specific transparency obligations, that they either inform users of the interaction with a machine, or they pose no risk (like spam filters).

The priority is, reasonably, set on the regulation of matters that are highly sensitive. The higher the risk, the higher the regulation. The generic obligation observes that most of AI is not considered as high-risk. Only transparency obligations are set (art. 52) and voluntary AI Codes of conduct are set for specific transparency requirements (art. 69).

For less or minimal risk, systems will have to warn users about the interaction with artificial intelligence, as well as the collection and treatment of emotion recognition or biometrics and the use of AI to portray human or human-like images (deep fake technology).

The draft regulation proposes for the high-risk systems to perform “conformity assessments” (algorithmic impact assessments, comparable to the current privacy impact assessments of the data protection industry) that will evaluate (prior to any deployment) the potential consequences on users and the ecosystem. Systems will also need to be explainable and subject to human oversight and companies will have to implement robust cyber risk management compliance procedures.

Another interesting characteristic will be the interjurisdictional reach of the proposed legislation, a move that almost mimics the current European Union’s General Data Protection Regulation (GDPR). Regardless of the location of the provider, any AI system interacting within the European Union will be subject to these rules.

Finally, potential sanctions and enforcement will be established around €30 million or 6 percent of global revenue, a step higher than GDPR, but using similar sanctions criteria.

We Are Not Entering Uncharted Territory

Since 2018’s implementation of GDPR, companies have begun to rhyme compliance with performance. Consequently, the future AI regulation will require companies to -sooner or later- begin to integrate these principles as a way to integrate and promote an AI Compliance culture in within the structure. The French Data Protection Agency (CNIL) has already stated the importance of a reasonable (and evident) articulation with GDPR principles as well as a robust integrated governance of the data.[5]

An AI inventory will probably become the go-to measure to (at least) understand the current presence of AI in the system, as well as establishing a clear risk-mapping strategy and the integration with all compliance mechanism related to data protection and cyber security.

We welcome this future regulation, and we understand that the best way to increase versatility of AI will be to allow a from-the-ground-up regulation that properly accompanies businesses, users, and governments in the creation of a universal and accountable artificial intelligence.

Published on : Sun, 5 Dec 2021