BULLETIN

EU Proposes Artificial Intelligence Regulation

Stefania Kolarz, Oskar Szydłowski

The proposed regulation of artificial intelligence (AI) on the EU market is primarily intended to protect fundamental rights and values. As the first regulation of this type in the world, it may set the standard. However, the new requirements in practice might hinder the access of foreign entities to the internal market and reduce the competitiveness of EU businesses.

On 21 April, the European Commission (EC) proposed a set of rules that would be the world's first project to comprehensively regulate AI. Until now, individual norms have only been adopted at the national level (e.g., definition of computer-generated work in UK legislation or the requirement in German law for a driver to be present in an autonomous vehicle). EU countries more often use political documents, such as strategies on AI (France, Estonia, Poland, Germany, among others). Following the General Data Protection Regulation (GDPR), the Union once again has the chance to set a global normative standard.

Key Assumptions. The regulation is aimed to ensure that ethics, security, EU values, and fundamental rights are respected in the creation of AI. The fixing of legal certainty should foster investment and AI development in the EU, strengthen the Union's competitiveness, and protect its digital sovereignty.

The draft provides for harmonised rules for the development, marketing, and use of AI in the EU. It is based on the division of AI systems into unacceptable, high, low, and minimal risk variants. The first category pertains to systems employing subliminal techniques intended to influence a person's behaviour in a harmful way, or uses social scoring. The project regulates most extensively high-risk AI systems, operating, for example, in the areas of transport, assessments of loan applications, or decisions granting social benefits. AI systems will have to meet a number of requirements, including appropriate testing, an assessment of compliance with EU standards, registration in an EU database, and proper care of user information. These obligations will apply to manufacturers and suppliers of AI systems, regardless of whether they are based in the Union or outside, as well as to users of such systems within the EU. In the case of other AI systems (e.g., chatbots), the proposal primarily creates an obligation to inform users that they are interacting with AI.

Non-compliance with the regulations will be subject to an even higher penalty than in the case of the GDPR—up to 6% of a company's total worldwide annual turnover. In the Member States, responsibility for implementation of the regulation will be designated by the national authorities. At the EU level, those national supervisors will form the European Artificial Intelligence Board (EAIB) with the European Data Protection Supervisor (EDPS), chaired by the Commission. The EAIB's task will be to advise the EC and coordinate the activities of the Member State AI authorities.

Regulation in Practice. The draft is supported by the EDPS, though it is insisting on an even stricter approach. While a few Member States, Germany, for example, favour broad regulation, many fear a slowdown in technological development. In the EU, 14 countries, including Poland, support limiting AI regulations to the necessary minimum or using non-binding instruments.

The proposal contains many exemptions and imprecise definitions. For example, the prohibition on biometric real-time identification only applies to law enforcement agencies in public spaces. It will thus not cover private spaces and other public bodies or private entities. Moreover, it will not apply when a system is to be used to counter terrorism or threat to the life or safety of people, which leaves a lot of room for interpretation.

The risk categorisation was prepared by the EC, but the criteria are not explicit. For example, risk assessment

method includes an appraisal based on applicability, which is vague. Since the models can be adapted to any application, the evaluators have a lot of grey area to justify each opinion. This could create unstable conditions for the development of AI, as the risk categories can be freely updated by the EC, affecting future applications. For example, so-called black box systems—functioning without human input—are qualified as high-risk. In "normal" models, the algorithm by which the model is to learn is specified. In the case of black boxes, the AI independently defines the variables and their weights, such as which data to omit (as the system makes its own decisions, it is difficult if not impossible to determine from the outside which variables were used, how, and why). They are highly effective (fit to purpose), but do not meet the risk-analysis requirements. Their qualification is a significant limitation of innovation in the EU.

Although the proposal claims the primacy of individuals over technology, it does not take into account the perspective of users of AI systems. In particular, there are no particular legal remedies, for example, a special mechanism for applying for compensation as a result of unauthorised or unforeseen operation of an AI system.

The International Dimension. The proposal would make it the most far-reaching regulation of AI in the world. However, it fits in with trends visible in other countries, particularly with respect to the emphasis on analysis of risks and threats related to AI and the preparation of action plans in case of violations. AI systems should be independently tested in real time, both during operation and after, due to the increasing and changing risk over time. This approach is comparable to local regulations, such as in the U.S. states of Virginia and California. Common rules provide a potential basis for negotiating regulations in a transatlantic format. However, it is unlikely that the U.S. will accept the EU's definition of high risk or an extensive technology monitoring system. The cooperation could benefit from already developed practices, such as mutual recognition of regulations and admission of entities to both markets. The willingness to cooperate is evidenced by the positive U.S. reception of the EU project by National Security Advisor Jake Sullivan.

American technology companies, including Google and Microsoft, have already announced they will challenge the EC proposal in court. Their existing AI systems have been largely trained on data from EU citizens. Many of them are also directly used in services offered on the EU market. This means that the regulation will force these companies to implement all risk-analysis mechanisms. Moreover, it will not be possible to bypass the requirements by spreading AI systems across separate companies operating outside the EU market because that will also be covered by the regulation. As a result, some of the services may not be offered in the EU, or special AI models dedicated to its market will be created. The resulting entry barrier will be daunting, only overcome by large companies. Additional obligations may further hinder the development and expansion of AI to foreign markets as significant resources will be allocated to meeting the new requirements, similar to the GDPR. Some AI applications, such as those using biometrics, will be completely banned in the EU, and as a result—assuming no similar global regulation—American and Chinese companies will quickly move to the fore.

Conclusions and Perspectives. The EU regulation of AI may follow the success of the GDPR as the world's first comprehensive set of rules governing the emerging technology. The EC assumes flexibility, planning to adjust to potential developments in the field of AI without the need for regular amendments. However, the regulation may also slow the pace of AI development and reduce the competitiveness of EU businesses. Despite the Member States' assistance to small and medium-sized enterprises envisaged in the draft (e.g., priority in access to special testing environments, easier access to information on the application of new regulations and lower costs of compliance assessment), the regulation may hinder access to the common market for businesses, including Polish firms.

The proposed regulation is needed from the point of view of human rights protection, but it should be adjusted to the real possibilities for enforcing compliance. To maximise its effectiveness without sacrificing the Union's competitive advantages, during EU-wide consultations the EC should simultaneously encourage foreign partners (e.g. the U.S.) to adopt similar AI standards, including with regard to protection of human rights, and at the WTO or OECD forum. At the Union level, additional support for companies registered in the EU could come through the creation of new programmes for financing AI research from Union funds.