



The Omnibus AI package weakens EU artificial intelligence regulation

Aleksandra Wójtowicz

On 16 June this year, the European Parliament voted to adopt the Omnibus AI package. It is an amendment to the Artificial Intelligence Act intended to become part of a broader programme of simplifying digital regulation, one that reduces the liability of AI system providers. Adopted under pressure from the United States and American technology companies, in effect, the package weakens the EU's position as a body setting global standards for regulating digital matters. Contrary to its intentions, the adoption of the package may negatively affect both European companies and the EU's competitiveness.

Political context. The Digital Omnibus on AI is not merely a correction to the AI Act but an element of a broader deregulatory turn in EU economic policy. Although efforts to reduce regulatory burdens have been present in the EU since the early 2000s, the [reports commissioned by the European Commission](#) from Mario Draghi and Enrico Letta initiated a new phase of these efforts and became the starting point for a new economic policy. According to the conclusions the Commission drew from both reports, the costs to the private sector of complying with the requirements imposed by EU regulation are too high, and excessive regulation harms the EU's competitiveness. On this basis, the Commission presented a series of Omnibus packages aimed at simplifying European regulation, including in the areas of climate, environmental reporting, and digital matters.

The push for deregulation has been reinforced by external pressure. The US has openly criticised EU digital regulation as harmful to its interests, viewing the rules as a direct attack on American technology companies. The US has backed this criticism with threats to impose high tariffs, a move that coincides with EU fears around a weakening of the American military presence in Europe. At the same time, pressure from the technology sector (including Microsoft, OpenAI, Meta, and X) is growing, as it actively works against digital-sector regulation in the EU. According to a Corporate Europe Observatory report, the digital industry's spending on lobbying in Brussels rose by more than 33% over two years,

to EUR 151 million annually. Deregulation is also favoured by some member states, including Poland and Denmark.

AI regulation in the EU. Even before entering into force, the Artificial Intelligence Act, the first EU regulation governing AI, was weakened by the Omnibus package, and the regulation is still awaiting full implementation. The Act imposes various obligations on AI providers depending on the potential risk associated with a given model, ranging from transparency requirements to obligations concerning risk management and data quality. Based on classifying AI according to the potential threats it could cause in the real world, the Act defines four tiers, covering unacceptable, high, medium, and low risk.

AI models assessed as unacceptable include systems used for "social scoring" (the automated rating of citizens by algorithms and artificial intelligence based on their behaviour), online activity, or finances. High-risk systems are those that affect fundamental rights, safety, or a person's life chances. These include tools for recruiting job candidates, determining eligibility for public benefits, or assessing creditworthiness. Limited-risk systems interact with people in ways that may be misleading; they include voice assistants and content generators. For these, the Act imposes above all transparency obligations—the user must know they are talking to a machine, and AI-generated content should be clearly labelled.

Drafted during the previous Commission's term, the AI Act was criticised as an example of overregulation even before it was adopted. In the new term, the Commission has identified artificial intelligence as a matter of key importance for the EU, in the belief that leadership in AI will determine economic competitiveness and global standing. As a result, in the Commission's view, a system imposing obligations on European AI developers became not only an economic burden but also a strategic one.

To actually implement the AI Act's provisions on high-risk systems, technical norms and standards were needed, and these were established by the European Committee for Electrotechnical Standardization, among others. These were not, however, delivered on time, which caused the Act to only partially enter into force, and jeopardised implementation of the provisions on high-risk systems.

Changes introduced by the Omnibus. The most significant change introduced by the Omnibus is the postponement of obligations for high-risk systems referred to in the AI Act. Originally, these were to begin taking effect from August this year, but under the new provisions, AI systems affecting fundamental rights will have to meet the requirements by 2 December 2027, and by 2 August 2028 for systems embedded in regulated products (that is, AI systems used in other products, e.g. in industry, transport, or healthcare). Systems subject to obligations of transparency and of labelling AI-generated content will receive additional time, with a deadline of 2 December this year.

The Omnibus also expands the possibility of using sensitive personal data to detect bias in AI systems. This allows developers of AI systems to legally use, among other things, information about race, origin, health, or sexual orientation, but solely for a strictly defined purpose: to detect *bias* in algorithms. Until now, this was permissible only for providers of high-risk systems; after the changes, it will be open to all AI systems. The Omnibus therefore conflicts with existing obligations under the GDPR, and these solutions have raised concerns among non-governmental organisations. In a letter to the European Commission signed by representatives of 130 NGOs, the Omnibus project was described as the largest dismantling of fundamental digital rights in EU history. In the trilogue, however, the EU institutions held that reducing bias in artificial intelligence models constitutes a legitimate public interest comparable to the protection of personal data.

The change in the liability of AI model providers is also important. Originally, high-risk systems were required to be

free of bias; now, platforms are merely obliged to take measures that limit bias in their models. The same applies to the obligation to ensure AI literacy. Under the AI Act, this was an obligation for digital platforms, but the Omnibus replaced it with a commitment by AI system providers to promote the knowledge and skills needed for the safe use of artificial intelligence tools—that is, AI literacy.

At the same time, the Omnibus broadens the catalogue of prohibited practices to include systems generating non-consensual sexual content. This is a direct response to the scandal surrounding Grok AI—a tool that generated pornographic content, including child pornography, and allowed it to be shared further on X.

Conclusions. The Digital Omnibus on AI is burdened by a procedural deficit: it was created without a full regulatory impact assessment and without the required public consultations, and it revised an act whose key provisions had not yet begun to apply. Any assessment of how it functions is, therefore, by definition, premature.

The Omnibus fits into a broader trend of deregulation that, contrary to its intentions, does not strengthen European competitiveness but instead delivers benefits to American big tech. The failure to implement the Artificial Intelligence Act's provisions on time has actually introduced greater instability into the market. The main beneficiaries of the postponements and relaxed obligations are the largest AI system providers, almost exclusively American—they lobbied most strongly for the changes, and their models dominate the high-risk applications segment. By contrast, European companies have lost the predictable regulatory environment that they had invested in, along with the potential competitive advantage that comes from certified compliance with the highest standards.

The Omnibus significantly weakens the EU's influence over the regulation of AI systems both internally and internationally. The "Brussels effect," by which EU rules and legal standards become de facto global norms, loses much of its effect when the EU's own legal acts are compromised. Having created one of the world's first cross-cutting pieces of AI legislation, the EU is now failing to actually implement it. Softening the AI Act will have a negative impact on the EU's other digital regulations and on its ability to shape global standards. A decline in the EU's role in setting legal norms will mean that the US, China, and other actors may begin to shape those norms, without taking into account the protection of fundamental rights or European values.