THE AI ACT HAS BEEN ENACTED: THE ARTIFICIAL INTELLIGENCE BETWEEN INNOVATION AND PROTECTION OF FUNDAMENTAL RIGHTS

On 13 March 2024, the European Parliament approved the "AI Act", which is intended to regulate certain applications of artificial intelligence systems for the first time. To ensure the safe use of artificial intelligence, the European legislator also provided for the establishment of the AI Office within the European Commission.

The Regulation will enter into force twenty days after its publication in the Official Journal of the European Union and will begin to apply two years after such publication, with certain exceptions. Prohibitions on prohibited practices will apply six months after the entry into force of the AI Act. There will also be a period of voluntary compliance (AI Pact), which will allow companies to comply with the Regulation before it comes into force.

Not only is the AI Act the first piece of legislation of its kind in the world, but it has also managed to strike a balance between innovation and the protection of fundamental EU rights, using a 'risk-based' approach.

Artificial intelligence systems will be categorized according to their risk profile: unacceptable risk, for systems expressly forbidden by the regulation; high risk, for systems that will be subject to an evaluation; low risk, for systems subject only to transparency obligations; minimal risk, for systems exempt from obligations.

The systems expressly prohibited are those used for:

a) categorizing people on the basis of sensitive characteristics, such as ethnicity, political or religious beliefs;

b) untargeted *scraping* of images. It is therefore prohibited to collect images from the Internet or from CCTV cameras to create a recognition *database* without specific targets;

c) recognizing emotions in workplaces or educational institutions;

d) *social scoring* and/or manipulative techniques;

e) target vulnerable people;

f) predictive policing.

For law enforcement agencies, in particular, some special instructions have been provided: exceptions have been made for biometric recognition, whi-

ch may be used in the case of an imminent terrorist threat or to search for a convicted person or a person suspected of committing a serious crime. In such cases, however, law enforcement agencies will have to notify the use of artificial intelligence to the authorities responsible for controlling it, who will monitor its use. In the case of the use of artificial intelligence systems to analyze crime data, moreover, such systems must operate on anonymous data and must not be used to profile specific individuals.

High-risk systems, on the other hand, are those that may affect citizens' fundamental rights: think, for instance, of artificial intelligence systems for assessing electoral behavior. For such systems, not only is it expected that the relevant manufacturers provide detailed technical documentation, including all operational processes and security measures used, but also that the systems undergo a fundamental rights impact assessment (to avoid compromising fundamental rights) and are subject to human supervision.

In any case:

- artificial intelligence systems, during their training phases, will still have to comply with EU copyright law;

- artificial or manipulated images and audio/video content (so-called *deepfakes*) should be clearly labelled as such;

- citizens are given the opportunity to complain about decisions taken using high-risk systems.

In addition to regulating the use of artificial intelligence systems, the AI Act has also taken care to provide for regulations to encourage the development of this sector. In fact, provision has been made for the creation of regulatory *sandboxes*, environments in which companies can experiment with artificial intelligence solutions under real-life conditions, with the possibility of benefiting from exemptions from industry regulations. In addition, specific exceptions have been provided for small and medium-sized enterprises to facilitate their adaptation to the new regulatory provisions.

It is also worth mentioning the system of sanctions provided for in the Regulation in the event of violation of its rules.

The penalties under the AI Act vary according to the seriousness of the violation and the size of the company:

a) for violations relating to prohibited practices or non-compliance with data requirements, there are penalties of up to EUR 35 million or up to 7 per cent of the total annual turnover of the previous financial year;

b) for failure to comply with any of the other requirements or obligations of the regulation, including violation of the rules on artificial intelligence models for general use, penalties may amount to up to EUR 7.5 million or 1.5 per cent of the total annual turnover in the previous financial year;

c) if, following a request by the competent bodies, inaccurate, incomplete,

or misleading information is provided, penalties can be up to EUR 7.5 million or 1.5 per cent of the total annual turnover of the previous financial year.

Finally, it should be noted that the AI Act has introduced several significant obligations directly affecting high-risk AI providers; among the main ones are:

a) ensure compliance with the specific technical requirements set out in the Regulation, provide essential information on the system, have a quality management system in place, draw up an EU declaration of conformity, take corrective measures if necessary and provide all the information required to the competent authorities;

b) take appropriate technical and organizational measures for compliant use, entrust the human supervision of the systems to competent persons, monitor the operation of the systems and cooperate with supervisory and control authorities.

For providers of general-purpose artificial intelligence models (including large generative artificial intelligence models), there are also specific obligations, including drawing up, keeping up-to-date and making available to the public the technical documentation of the model, including details of the model's training and testing process, as well as the results of its evaluation.

For importers and distributors of artificial intelligence, on the other hand, these obligations only apply if they have put their name or trademark on the system after it has already been placed on the market, if they have made substantial modifications after it has been placed on the market (provided that the system remains high-risk), or if they have changed the intended purpose of the artificial intelligence system by making it high-risk.

DISCLAIMER
The sole purpose of this *Client Alert* is to provide general information. Consequently, it does not represent a legal opinion nor can it in any way be considered as a substitute for specific legal advice.

Paola Sangiovanni, Partner
Email: paola.sangiovanni@grplex.com

Falvio Monfrini, Partner
Email: flavio.monfrini@grplex.com

Marco Blei, Counsel
Email: marco.blei@grplex.com

Arianna Rizza, Junior Associate
Email: arianna.rizza@grplex.com