TopHic | dig deeper

May 2025

AI Act: risks and opportunities

Expert's opinion

DPO's role in AI Act era

*by **Guglielmo Troiano***

Lawyer – Grant Thornton Financial Advisory Services

In this initial phase of enforcement of the AI Act many organisations are struggling to find clear indications on who will have to oversee the compliance with the new regulations. The lack of roles formally provided by the UE legislation for the internal governance of AI systems generates an operational void that risks translating into inefficiencies or disorganised approaches. The figure of the Chief Artificial Intelligence Officer (CAIO) is often evoked in the debate, but to date it appears more like a theoretical construct than a function that can actually be implemented in business organisations. In this scenario, the DPO appears as a reference point that has been present in companies for years, equipped with a transversal vision and regulatory skills that, although not exhaustive, can be enhanced to...

read more

Overview

A European regulation for ethical and secure AI

*by **Renato Sesana***

Partner - Grant Thornton Financial Advisory Services

The AI Act – Regulation (EU) 2024/1689 – is the first global regulation on artificial intelligence and could become a global reference standard. The aim of this regulation is that of making the European Union a world leader in the adoption of anthropocentric and reliable artificial intelligence. To do this, legislation must be harmonized between Member States, establishing a uniform legal framework regarding the development, launching, commissioning, and use of artificial intelligence systems within the EU. All this, while ensuring high protection of health, safety and fundamental rights sanctioned in the European Charter of Fundamental Rights. Artificial intelligence started being used in key sectors for...

read more

Focus on

Machina delinquere potest?

*di **Silvia Laura Rossi***

Lawyer – Grant Thornton Financial Advisory Services

Addressing the topic of artificial intelligence in businesses leads us to think from an integrated compliance perspective, also with reference to the various figures involved. It can be stated that the higher the risk rating of an artificial intelligence system in undermining the fundamental rights on which the European Union is founded, the more stringent the obligations to be complied with become. Similarly, the same ratio underpins the provisions of Legislative Decree no. 231/2001, mandatorily requiring companies to identify, assess and manage the risks of predicate offences within their activity, through the implementation of a robust and effective internal control system. Public and private companies increasingly making use of software and AI systems lead to...

read more

Supplemento Notizie flash n° 107 del 25 febbraio 1984

Grant Thornton

Overview

A European regulation for ethical and secure AI

by ***Renato Sesana***
Partner - Grant Thornton Financial Advisory Services

The AI Act – Regulation (EU) 2024/1689 – is the first global regulation on artificial intelligence and could become a global reference standard. The aim of this regulation is that of making the European Union a world leader in the adoption of anthropocentric and reliable artificial intelligence. To do this, legislation must be harmonized between Member States, establishing a uniform legal framework regarding the development, launching, commissioning, and use of artificial intelligence systems within the EU.

All this, while ensuring high protection of health, safety and fundamental rights sanctioned in the European Charter of Fundamental Rights. Artificial intelligence started being used in key sectors for the Italian economy, contributing to facing some of the most urgent challenges of our times. Given the ongoing revolution, the European legislator has adopted, as it has been common to all recently issued "technical" regulations, a risk-based approach: therefore, the higher the risk in the use of a certain AI system, the higher the responsibilities of those who develop, release, and use that specific system, up to setting a prohibition to use those applications and technologies whose risk is considered unacceptable. The risk classification system aims to balance technological innovation with people protection, ensuring a responsible use of artificial intelligence.

Expert's opinion

DPO's role in AI Act era

by ***Guglielmo Troiano***
Lawyer - Grant Thornton Financial Advisory Services

In this initial phase of enforcement of the AI Act many organisations are struggling to find clear indications on who will have to oversee the compliance with the new regulations. The lack of roles formally provided by the UE legislation for the internal governance of AI systems generates an operational void that risks translating into inefficiencies or disorganised approaches. The figure of the ***Chief Artificial Intelligence Officer*** (CAIO) is often evoked in the debate, but to date it appears more like a theoretical construct than a function that can actually be implemented in business organisations. In this scenario, the DPO appears as a reference point that has been present in companies for years, equipped with a transversal vision and regulatory skills that, although not exhaustive, can be enhanced to provide an initial response to compliance needs.

Although not explicitly provided for within the AI Act, the DPO can be considered as a "natural" extension towards AI, especially with regard to the requirements of transparency, traceability, documentation and human oversight. Even though this extension is not without critical aspects - the DPO remains formally responsible for monitoring compliance with the GDPR, not for all of the provisions of the AI Act - it represents to date a pragmatic solution, pending the definition of more structured and sector-specific roles.

It is true that the AI Act introduces obligations that go beyond the scope of personal data protection, touching on complex technical and organisational aspects. Anyway, just because of their experience in risk assessment, document management and the promotion of practices inspired by the principle of accountability, DPOs can effectively contribute, right from the start, to the integration of AI requirements into existing business processes, acting as a link between regulatory compliance and operational governance.

The risk of functional ambiguities, if not clearly governed, remains real: it is crucial that the DPO involvement does not turn into an improper delegation or an overload of responsibilities in areas that require interdisciplinary skills. However, if supported by adequate structures and complementary professionals (e.g. AI experts, risk management and applied ethics), the DPO can act as a catalyst for internal processes aimed at compliance, contributing to the definition of policies, integrated impact assessments and proportionate audit mechanisms.

In conclusion, far from being granted a regulatory centrality that they do not currently possess, DPOs can still play an active, realistic and supervisory role in the implementation of the provisions of the AI Act. Pending the definition of new institutional figures responsible for the supervision of artificial intelligence systems, their contribution represents a precious resource for a transitory but responsible governance, upon condition that the relevant limits are respected and specific skills valued.

Focus on

Machina delinquere potest?

by ***Silvia Laura Rossi***
Lawyer – Grant Thornton Financial Advisory Services

Addressing the topic of artificial intelligence in businesses leads us to think from an integrated compliance perspective, also with reference to the various figures involved.
It can be stated that the higher the risk rating of an artificial intelligence system in undermining the fundamental rights on which the European Union is founded, the more stringent the obligations to be complied with become. Similarly, the same ratio underpins the provisions of Legislative Decree no. 231/2001, mandatorily requiring companies to identify, assess and manage the risks of predicate offences within their activity, through the implementation of a robust and effective internal control system.

Public and private companies increasingly making use of software and AI systems lead to an in-depth reflection on how – and to which extent – the use of such tools may concretely facilitate the commission of specific predicate offences, exposing companies to the risk of potential liability.

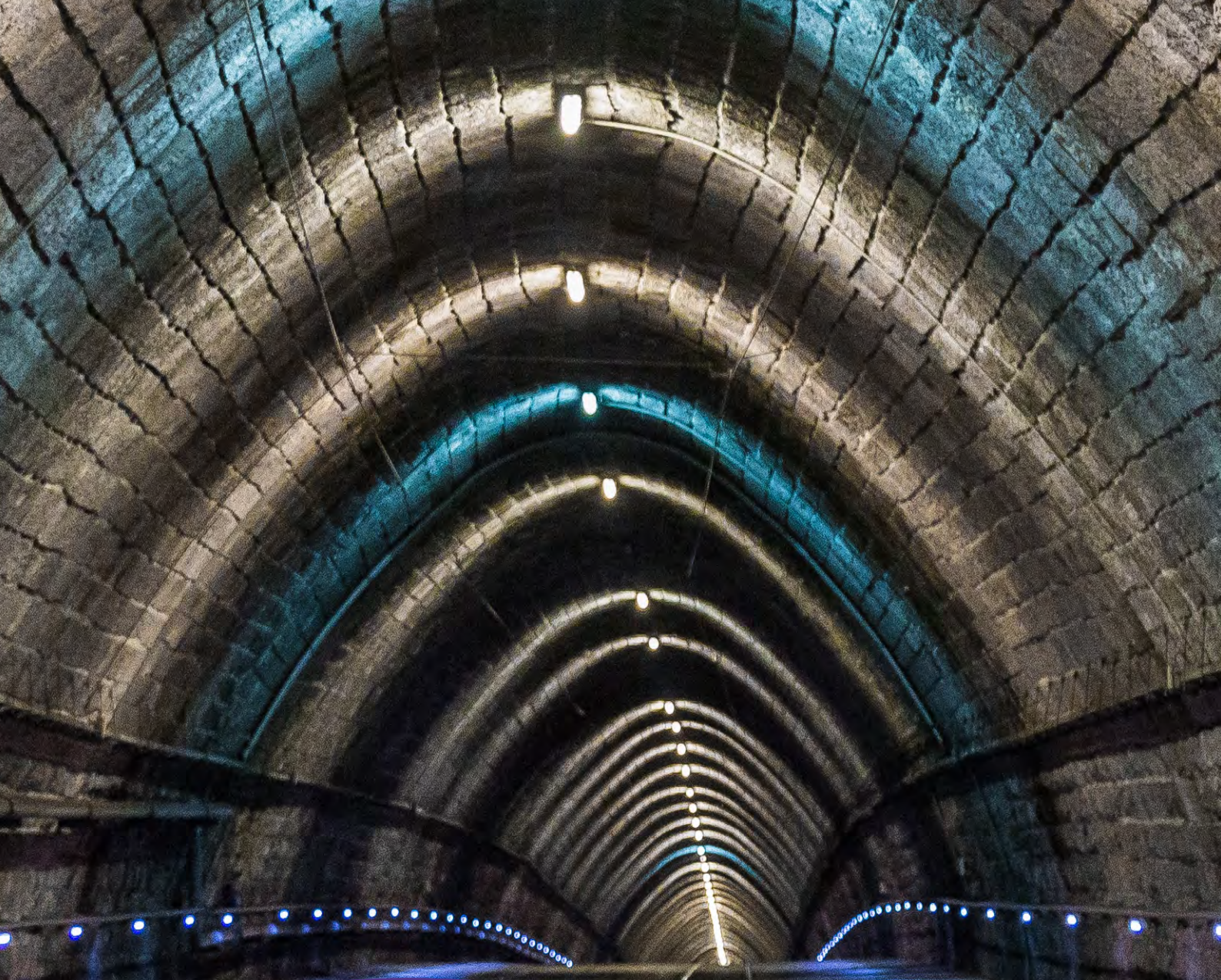
Just think about money laundering, which may be favoured by automated payment systems allowing anonymous transactions between different bank accounts, cryptocurrencies or digital platforms.

Therefore, when setting up an internal control system, the implementation of procedural rules not only aimed at complying with the provisions of the AI Act – differentiated based on the risk assessment attributed to AI systems – but also suitable to monitor the previously identified offence risks cannot be disregarded.

Both regulations thus consider preliminary risk monitoring ethics as the key factor of risk management strategies.

The domestic legislator promptly intervened on this matter and with a draft law on artificial intelligence – currently being examined by the Chamber of Deputies – provided for a redefinition of the criteria for the attribution of an entity's liability considering the actual degree of control over AI by the operator. This relates to the principle of human surveillance, key element of the AI Act, i.e. devising and developing a system encompassing human supervision measures in order to guarantee that AI systems be effectively monitored by people during its use.

In order to support businesses in promoting a culture of lawfulness it is necessary to know and apply regulation with an integrated approach, so as to enhance synergies among the various regulatory frameworks.



Meet risks with confidence and transform your business

Grant Thornton