

Corporate Criminal Liability in Italy: new AI-related offences under Legislative Decree n. 231/2001

Authors: Avv. Francesco Attilio Bico, Avv. Jacopo Campiglio

Legislative Decree No. 231/2001 introduced a framework of corporate criminal liability into Italian law, formally classified as administrative liability, for offences committed in the company's interest or for its benefit by individuals in senior positions or persons subject to their direction or supervision. The Decree provides for a strict system of sanctions, including potentially substantial financial penalties and disqualifying sanctions that, in the most serious cases, may extend to a permanent ban on carrying on business activities. The Decree applies, currently, to a list of more than 200 criminal offences, ranging from bribery to health and safety or environmental infringements.

With the growing use of artificial intelligence systems, the Parliament considered it necessary to expand the list of offences giving rise to corporate liability by introducing two additional offences relating to the use of these technologies.

In this context, on 15 September 2026, Legislative Decree No. 160/2026 was published in the Italian "Gazzetta Ufficiale" under the title: *"Adaptation of national legislation to the provisions of Regulation (EU) 2024/1689 (AI Act) of the European Parliament and of the Council of 13 June 2024, establishing harmonized rules on artificial intelligence, with regard to the use of artificial intelligence systems in police work and civil and criminal liability."*

This legislation, which entered into force on 30 September 2026, formally brings certain additional offences relating to the use of AI tools within the scope of Legislative Decree



No. 231/2001, providing for substantial financial penalties and disqualifying sanctions against entities in whose interest and/or for whose benefit such offences are committed.

Specifically, Legislative Decree No. 160/2026 expands the list of so-called “offences” giving rise to corporate liability by introducing the new Article 25-vicies.

This article covers two separate criminal offences:

1. Article 612-quater of the Italian Criminal Code, entitled **“Unlawful dissemination of content generated or altered using artificial intelligence systems”**, which provides for imprisonment of between one and five years for: *“Any person who causes unjust harm to another person by transferring, publishing or otherwise disseminating, without that person’s consent, images, videos or voices falsified or altered through the use of artificial intelligence systems and capable of misleading others as to their authenticity.”*

This offence already exists under the Italian Criminal Code and, following the legislative amendment, is now expressly included among the offences that may give rise to corporate liability.

As can readily be inferred from a reading of the provision, this offence penalizes the creation of so-called “deepfake” content without the consent of the person concerned and capable of causing that person unjust harm.

Particular attention should therefore be paid to the Company’s functions responsible for promotional communications (marketing, social media, etc.), to prevent the external distribution of content that could potentially fall within the scope of this provision.

2. Article 437-bis of the Italian Criminal Code, entitled **“Failure to adopt safety measures in artificial intelligence systems”**, which provides as follows:



“Any person who fails to adopt the technical safety measures required for the design, training, production or placing on the market of high-risk artificial intelligence systems, suitable for preventing malfunctions or alterations to the operation of those systems, or who fails to adopt human oversight measures, shall be punished by imprisonment of between one and five years where such omissions give rise to a danger to life or to public or individual safety. Where the conduct gives rise to a danger to national security, the penalty shall be imprisonment of between two and eight years.

Unless the conduct constitutes a more serious offence, any person who, in circumstances other than those referred to in the first paragraph, alters high-risk artificial intelligence systems shall be punished by imprisonment of between two and six years where such conduct gives rise to a danger to life or to public or individual safety. Where the conduct gives rise to a danger to national security, the penalty shall be imprisonment of between three and ten years.

Where any of the acts referred to in the first paragraph is committed through gross negligence, the penalty shall be reduced by between one third and one sixth.

A professional user of high-risk artificial intelligence systems who intentionally fails to adopt human oversight measures shall be subject to the penalties laid down in the first and second sentences of the first paragraph where such omission gives rise, respectively, to a danger to life or to public or individual safety, or to a danger to national security.”

This is a newly introduced offence, added simultaneously to the Italian Criminal Code and to Legislative Decree No. 231/2001, which penalizes various forms of failure to adopt certain safety or human oversight measures in relation to so-called “high-risk” AI systems. As the final paragraph of the provision makes clear, users of AI tools may also commit this offence where they intentionally fail to adopt human oversight measures when using such systems and that omission gives rise to a danger to life, public or individual safety, or national security.



By way of example, “high-risk” AI systems include systems intended to be used for the recruitment or selection of natural persons, to place targeted job advertisements, to analyse or filter job applications and to evaluate candidates; to make decisions affecting the terms of employment relationships or the promotion or termination of employment contracts; to allocate tasks based on individual behaviour or personal traits or characteristics; or to monitor and evaluate the performance and behaviour of individuals within such employment relationships.

Particular care should therefore be taken in carrying out these activities, where the use of AI systems is permitted but only on the condition that human oversight measures are adopted.