

Artificial intelligence: Legislative Decree No. 160/2026 published on criminal liability and corporate liability for offences

1. Introduction

Legislative Decree No. 160/2026, which aligns Italian law with the AI Act, was published in the Official Gazette (*Gazzetta Ufficiale*) on 15 September 2026.

The Decree, which will enter into force on 30 September 2026, introduces into the Italian Criminal Code the new offence of “Failure to adopt safety measures for artificial intelligence systems and unlawful alteration of systems” (Article 437-bis of the Criminal Code), which is also a predicate offence for the purposes of corporate liability under the new Article 25-vicies of Legislative Decree No. 231/2001, together with the offence relating to so-called “deepfakes” (Article 612-quater of the Criminal Code).

2. The new offence of failure to adopt safety measures for artificial intelligence systems and unlawful alteration of those systems (Article 437-bis of the Criminal Code)

The provision, as enacted, is structured as follows.

Failure to adopt safety measures (paragraph 1). A person who, in the design, training, production or placing on the market of high-risk AI systems, fails to adopt technical safety measures suitable to prevent malfunctions or alterations to the systems’ operation, or fails to adopt human oversight measures, is liable to imprisonment for one to five years where those omissions give rise to a danger to life or to public or individual safety. Where the act gives rise to a danger to State security, the penalty is imprisonment for two to eight years.

Unlawful alteration of systems (paragraph 2). Unless the act constitutes a more serious offence, a person who, outside the circumstances covered by paragraph 1, alters a high-risk AI system is liable to imprisonment for two to six years where the act gives rise to a danger to life or to public or individual safety. The penalty is imprisonment for three to ten years where the danger concerns State security.

Gross negligence (paragraph 3). If an omission covered by paragraph 1 is committed through gross negligence, the penalty is reduced by between one sixth and one third.

Professional user (paragraph 4). A professional user of a high-risk AI system who intentionally fails to adopt human oversight measures is liable to the penalties provided for in the first and second sentences of paragraph 1 where the omission gives rise, respectively, to a danger to life or to public or individual safety, or to a danger to State security.

Both forms of the offence apply exclusively to high-risk AI systems, as classified under Article 6 of the AI Act. They are offences requiring a concrete danger: criminal liability depends on the conduct actually giving rise to a danger to the interests protected by the provision (life, individual or public safety, or State security). The penalties are graded according to the interests endangered, with heavier sentences where State security is at risk.

3. Amendments to legislative decree no. 231/2001: the new article 25-vicies

Article 15 of Legislative Decree No. 160/2026 inserts a new Article 25-vicies, headed “Offences committed using artificial intelligence systems”, into Legislative Decree No. 231 of 8 June 2001. In its final form, the provision identifies two predicate offences:

- the offence under the new Article 437-bis of the Criminal Code (failure to adopt safety measures for AI systems and unlawful alteration of those systems), for which the legal person is subject to a monetary penalty of 600 to 1,000 quota units;
- the offence of unlawful dissemination of artificially generated or manipulated content, commonly referred to as “deepfakes” (Article 612-quater of the Criminal Code), introduced by Law No. 132/2025, for which the legal person is subject to a monetary penalty of 200 to 700 quota units.

In both cases, Article 25-vicies provides for the disqualifying sanctions listed in Article 9(2)(b)–(e) of Legislative Decree No. 231/2001: suspension or revocation of authorisations, licences or concessions instrumental to the commission of the offence; a prohibition on contracting with public authorities; exclusion from benefits, financing, grants or subsidies, including possible revocation of those already granted; and a prohibition on advertising goods or services.

The decision to place these new predicate offences in a separate Article 25-vicies, instead of including them in the existing Article 24-bis on cybercrime, confirms that artificial intelligence is now treated as a distinct area of organisational risk for the purposes of Legislative Decree No. 231/2001.

4. Implications for updating 231 compliance models and for the supervisory body

The entry into force of Article 25-vicies requires legal persons that use AI systems to assess its implications for their organisational, management and control model under Legislative Decree No. 231/2001 (the “231 Model”). Merely adding the new predicate offences to the model will not suffice.

The first step is to take an inventory of the AI systems actually in use, identify the legal person’s role in the supply chain (provider, importer, distributor or deployer), and determine whether any of the systems qualify as “high-risk”. Particular attention should be paid to the design, training, production, placing on the market and professional use activities referred to in Article 437-bis of the Criminal Code.

The legal person must then map the processes and activities exposed to risk, taking account both of the new offences and of the possibility that the AI tools identified could be used to commit other predicate offences already covered by Legislative Decree No. 231/2001. In this respect, AI may be a means of committing various 231 predicate offences, in addition to the offences under Articles 437-bis and 612-quater of the Criminal Code.

Once the risks relevant under Legislative Decree No. 231/2001 have been mapped, the adequacy of existing controls should be reviewed and any gaps addressed. Human oversight is a key safeguard: the responsible persons, their skills, the points at which they intervene and the documentary record should all be identified. With regard to Article 612-quater of the Criminal Code, procedures for using generative AI to produce content that may be manipulated (deepfakes) should also be regulated.

Lastly, corporate training programmes must be updated to ensure that personnel understand the capabilities and limitations of AI systems and the responsibilities associated with their use. This should address the AI literacy

obligation already set out in Article 4 of the AI Act and include specific training on the risk of committing predicate offences under Legislative Decree No. 231/2001.

The Supervisory Body (*Organismo di Vigilanza*, or “OdV”) will need to oversee these measures, calibrating its review to the entity’s actual exposure to risk.

Together, these measures can reduce the risk of offences being committed through the use of AI systems. They also allow the entity to establish a robust defence by demonstrating the reasonable steps it took to prevent such offences, whether the allegations concern Articles 437-bis and 612-quater of the Criminal Code or other predicate offences committed using AI systems.

This document is delivered for informative purposes only.
It does not constitute a reference for agreements and/or commitments of any nature.
For any further clarification or research please contact:

Ciro Pellegrino
Partner

Head of White Collar Crime Department
Rome
+39 06 478751
cpellegrino@gop.it

Fabio Ilacqua
Partner

Head of New York Office
Corporate/M&A
+1 212 957 9600
filacqua@gop.it



INFORMATIVA EX ART. 13 del Reg. UE 2016/679 - Codice in materia di protezione dei dati personali

I dati personali oggetto di trattamento da parte dallo studio legale Gianni & Origoni (lo “Studio”) sono quelli liberamente forniti nel corso di rapporti professionali o di incontri, eventi, workshop e simili, e vengono trattati anche per finalità informative e divulgative. La presente newsletter è inviata esclusivamente a soggetti che hanno manifestato il loro interesse a ricevere informazioni sulle attività dello Studio. Se Le fosse stata inviata per errore, ovvero avesse mutato opinione, può opporsi all’invio di ulteriori comunicazioni inviando una e-mail all’indirizzo: relazioniesterne@gop.it. Titolare del trattamento è lo studio Gianni & Origoni, con sede amministrativa in Roma, Via delle Quattro Fontane 20.