INSIGHT | september 29th, 2026

Artificial intelligence: legislative decree 160/2026 enters into force on 30 september. New criminal liability and “231” liability in the use of AI systems

Legislative Decree No. 160 of 9 September 2026 will enter into force on 30 September 2026. It was adopted in implementation of Law No. 132/2025 on “*Provisions and delegations to the Government on artificial intelligence*” and published in Official Gazette No. 214 of 15 September 2026.

The Decree aligns national legislation with Regulation (EU) 2024/1689 (the AI Act), with specific reference to the use of artificial intelligence systems in police activities, and introduces significant changes concerning **criminal and civil liability**, also amending the system of **administrative liability of entities under Legislative Decree No. 231/2001**.

The final text completes the process begun on 10 June 2026 with the preliminary approval of the draft **legislative decrees; the separate process concerning the powers of the national Authorities and AI training remains distinct.**

For businesses, the Decree makes it necessary to assess not only the technical compliance of AI systems, but also the **adequacy of organizational safeguards**, security measures, human oversight mechanisms, documentation and the **231 Model** in light of the new risk profiles.

The new liability framework

The Decree operates along **three main lines:**

- regulation of the use of AI in police activities;
- introduction of new criminal and procedural provisions, with direct implications for the liability of entities under Legislative Decree 231/2001;
- provision of specific civil procedural tools for actions seeking compensation for damage caused by the use of artificial intelligence systems.

Amendments to the Criminal Code: the new Art. 437-bis

Article 12 of the Decree introduces Art. 437-bis into the Criminal Code, entitled “*Failure to adopt security measures in artificial intelligence systems and unlawful tampering with such systems.*”

The provision distinguishes four scenarios:

- **Intentional omission of security or oversight measures:** the first paragraph punishes anyone who fails to adopt the technical security measures required for the design, training, production or placing on the market of high-risk AI systems, which are suited to preventing malfunctions or alterations of operation, or who fails to adopt human oversight measures. The penalty is imprisonment from one to five years where the omission gives rise to danger to public or individual life or safety, and from two to eight years where it gives rise to danger to State security;
- **Unlawful tampering with AI systems:** the second paragraph punishes, unless the act constitutes a more serious offence, anyone **who tampers with high-risk AI systems.** The penalty is imprisonment from two to six years if this gives rise to danger to public or individual life or safety, and from three to ten years if it gives rise to danger to State security;

- **Negligent omission of security or oversight measures:** the third paragraph makes the acts referred to in the first paragraph punishable in cases of gross negligence, with a reduction of the penalty provided for by that provision;

- **Intentional omission of oversight measures by the professional user:** the fourth paragraph punishes the professional user of high-risk AI systems who intentionally omits human oversight measures, where this gives rise, respectively, to danger to public or individual life or safety, or to State security.

Compared with the draft, the final text distinguishes more clearly between the parties involved at the various stages of the life cycle of high-risk AI systems and the professional user, for whom criminal liability for failure to provide human oversight is limited to intentional conduct.

Amendments to Legislative Decree 231/2001: the new Art. 25-vicies

Article 15 of the Decree introduces into Legislative Decree 231/2001 the new Art. 25-vicies, "*Offences committed through the use of artificial intelligence systems*", confirming the structure of the draft::

- for the offence under Art. 437-bis of the Criminal Code, the entity faces a financial penalty of 600 to 1,000 quotas;
- for the offence of unlawful dissemination of content generated or altered with artificial intelligence systems (so-called "*deepfakes*") under Art. 612-quater of the Criminal Code, already introduced by Law 132/2025, the financial penalty is 200 to 700 quotas;

in both cases, the disqualification sanctions under Art. 9(2) apply, in particular: (i) suspension or revocation of the authorisations, licences or concessions instrumental to the commission of the offence (letter b); (ii) prohibition on contracting with the Public Administration (letter c); (iii) exclusion from benefits and funding, with possible revocation of those already granted (letter d); (iv) prohibition on advertising goods or services (letter e).

For businesses, the introduction of the new predicate offence **makes it advisable to review the 231 risk mapping relating to AI systems**, with particular attention to high-risk systems, responsibilities across the system's life cycle, technical security measures, human oversight safeguards, and the traceability of decisions and controls.

Artificial intelligence in police activites

Title I of Legislative Decree No. 160/2026 regulates the use of AI systems by the police forces according to a **human-centred, proportionate and risk-based approach**. Under **Art. 3**, the systems and their outputs serve as a support to human activity: when the results of automated processing are used in acts or measures affecting the legal sphere of the persons concerned, **qualified and documented human review is required**. For high-risk systems, effective human oversight by adequately trained personnel must also be ensured.

Biometric identification and facial recognition

The Decree pays particular attention to **real-time remote biometric identification**, distinguishing between preventive and investigative purposes:

- for **preventive purposes, Art. 8** permits real-time remote biometric identification, in the cases specified by the provision, for the targeted search of specifically identified or identifiable persons. Its use is subject to **authorisation by the competent Public Prosecutor**, specifying the purpose, the territorial area, the persons concerned, the databases used and the duration, which may not exceed fifteen days, unless extended by reasoned decision. Specific procedures are provided for urgent cases;

- for **investigative purposes**, the new **Art. 359-ter of the Code of Criminal Procedure**, introduced by Art. 13 of the Decree, permits real-time biometric identification or location in expressly provided cases, including the search for persons suspected of certain offences, fugitives and specific victims. Its use is authorised by the Judge for Preliminary Investigations (GIP) upon request of the public prosecutor. In urgent cases, early activation is permitted, subject to subsequent validation.

These safeguards are accompanied by specific guarantees on **data processing**. In particular, the use of biometric databases populated through untargeted scraping is prohibited.

Art. 10 separately regulates **retrospective facial recognition** through **video surveillance** systems integrated with AI components. The technology may be activated only after the images have been acquired and, when used for the targeted search for a suspected person, authorisation by the GIP upon request of the

Public Prosecutor is required. An exception applies to use after the commission of the offence solely for the initial identification of a potential suspect on the basis of objective and verifiable elements connected to the offence.

For such systems, the Decree also provides for a **prior impact assessment**, retention of data for **seven days** and of logs for five years. No decision producing adverse legal effects may be based solely on the results of facial recognition, and any non-targeted use, or use aimed at generalised and indiscriminate biometric control or identification of persons, is prohibited.

What to do

Legislative Decree No. 160/2026 strengthens the need to **integrate AI governance with internal control systems and the 231 Model**. In particular, it appears advisable to:

- inventory the AI systems used by the organisation and verify their classification, with specific attention to high-risk systems;
- identify roles, responsibilities and control powers across the systems' life cycle, distinguishing the position of the professional user from that of other operators;
- verify and document technical security measures, human oversight mechanisms, escalation procedures and the traceability of interventions;
- coordinate AI governance with risk mapping and the 231 Model protocols, as well as with information flows to the Supervisory Body (Organismo di Vigilanza).

Overall, the published text confirms that AI compliance cannot be treated as a purely technical matter. The Decree directly links the security and oversight of AI systems to criminal and 231 liability. It is therefore on this **interplay between governance, responsibility and evidence** that businesses should now focus their attention.

Contacts

Giovanni Morgese
giovanni.morgese@lcalex.it

Paolo Erik Liedholm
paolo.liedholm@lcalex.it

Chiara Mammola
chiara.mammola@lcalex.it

MILANO
Via della Moscova 18
20121 Milano

ROMA
Piazza del Popolo 18
00187 Roma

GENOVA
Via XX Settembre 31/6
16121 Genova

TREVISO
Via Sile 41
31056 Roncade (TV)

BRUXELLES
Place Poelaert 6
1000 Bruxelles

DUBAI
IAA Middle East Legal Consultants LLP
Liberty House, Office 514, DIFC

www.lcalex.it
info@lcalex.it