

October 2026

Legislative Decree No. 160/2026: civil and criminal liability and remedies for AI-related damages

On 15 September 2026, Legislative Decree No. 160 of 9 September 2026 (the "**Decree**") was published in the Italian Official Gazette and entered into force on 30 September 2026. The Decree adapts the Italian legal framework to Regulation (EU) 2024/1689 (the "**AI Act**") in relation, on the one hand, to the use of artificial intelligence systems in law enforcement activities and, on the other hand, to the civil and criminal liability associated with the development and unlawful use of such systems.

In particular, the Decree introduces new procedural mechanisms applicable to claims for compensation arising from damage caused through the use of AI systems. These provisions are relevant to companies, professionals, public authorities and, more generally, any entity deploying AI systems in contractual or non-contractual activities.

New article 25-*vicies* of Legislative Decree No. 231/2001: corporate liability for AI-related offences

The new article 25-*vicies* of Legislative Decree No. 231/2001 extends corporate liability of legal entities to the offences set out in article 437-*bis* of the Italian Criminal Code, "*Failure to adopt safety measures for artificial intelligence systems and unlawful alteration of systems*" and article 612-*quater* of the Italian Criminal Code, "*Unlawful dissemination of content generated or altered through artificial intelligence systems*". These offences concern deficiencies in the security or oversight of high-risk AI systems and the unlawful dissemination of so-called deepfakes.

Companies should therefore assess, based on their specific exposure, whether updates to their risk assessment under their Organisational Model adopted pursuant to Legislative Decree No. 231/2001 are required, coordinating such review with their AI Act compliance framework and adapting internal controls and reporting mechanisms towards the Supervisory Body.

A dedicated procedural framework for AI-related damages

The new rules operate on two different levels: general provisions apply to all compensation claims relating to damage caused through the use of AI systems; enhanced protections, including the presumption of causation, apply only where one or more obligations under the AI Act have been breached.

Jurisdiction based on the injured party's residence: where a natural person acting for purposes outside their professional activity brings an action, jurisdiction also lies with the court of the claimant's place of residence or domicile.

Relationship with other legal frameworks: the protections available under the GDPR and under legislation governing liability for defective products remain unaffected.

Access to evidence and disclosure orders

In order to address the information asymmetry between an injured party and the entity controlling an AI system, courts may order a party or a third party to disclose evidence relevant to the functioning of the AI system where the claimant has substantiated the claim with specific facts and circumstances making it reasonably plausible.

Disclosure orders may cover, among other things, log records, documentation relating to the risk

management system, relevant information contained in technical documentation, and information relating to human oversight mechanisms. Disclosure must be necessary and proportionate and may be accompanied by measures aimed at protecting trade secrets and confidential information.

Where a party unjustifiably fails to comply with a disclosure order, the court may draw adverse inferences. In the case of specific technical documentation identified by the Decree, the facts alleged by the requesting party may be deemed admitted. In addition, a non-compliant third party may be subject to an administrative monetary penalty ranging from EUR 1,500 to EUR 10,000.

Presumption of causation

Where damage results from a breach of obligations imposed by the AI Act, the causal link between the breach and the damage is presumed unless proven otherwise. Accordingly, the claimant must establish the existence of the damage and the underlying breach, while the defendant bears the burden of demonstrating either that the breach did not cause the damage or the damage would have occurred regardless of the alleged breach.

The presumption is rebuttable and does not apply automatically to any damage associated with AI. The alleged infringement of the AI Act must be pleaded with sufficient specificity and must be causally relevant to the damage claimed.

Certified compliance and liability

Compliance with AI Act requirements, including compliance assessed through the conformity assessment procedures established by the Regulation, does not automatically exclude civil liability. Such compliance may be taken into account when assessing the overall conduct of the defendant, but it does not prevent courts from independently evaluating the existence of damage and the causal link between the damage and the use of the AI system.

Direct action against the insurer

The Decree introduces a direct right of action enabling injured parties to bring claims directly against the insurer covering the civil liability of the potentially liable party, within the limits of the applicable insurance policy. Although insurance coverage is not mandatory, injured parties may request information from the potentially liable party regarding the existence of insurance coverage applicable to the damage at issue.

The recipient of such request must respond within 30 days, indicating whether insurance coverage exists, the details of the policy and the identity of the insurer. Failure to respond, or providing an incomplete response, may be taken into account by the court when assessing the evidence.

The insurer may invoke against the injured party only those contractual defences that arose prior to the occurrence of the loss and retains any rights of recourse against the insured to the extent permitted under the insurance contract.

The allegedly liable party is a necessary party to the proceedings, and the limitation period applicable to the claim against the insurer corresponds to the limitation period applicable to the claim against the alleged wrongdoer.

Practical implications

The new framework significantly increases the importance of technical and organizational traceability of AI systems. In anticipation of potential claims, companies and professionals should ensure consistency between regulatory requirements, internal processes, document management practices and insurance coverage.

- Mapping all AI systems used, identifying their purposes, relevant stakeholders and classification under the AI Act.

- Retaining logs, technical documentation, risk assessments and records relating to human oversight activities in a complete and readily accessible manner.
- Implementing internal procedures for handling disclosure requests while balancing procedural cooperation, data protection requirements and trade secret protection.
- Reviewing existing civil liability insurance policies, paying particular attention to the scope of coverage, exclusions, limits of indemnity and disclosure obligations relating to AI-related risks.
- Based on the mapping exercise, assessing criminal liability risks and align AI Act compliance measures with the Organizational Model adopted pursuant to Legislative Decree No. 231/2001 and the related reporting flows to the Supervisory Body.

In light of the new evidentiary rules and the availability of direct actions against insurers, proper document retention and timely review of insurance coverage become increasingly important tools for both preventing and managing litigation.

The Firm remains available to assist companies and professionals in assessing the impact of the Decree, reviewing documentary and organizational safeguards, and analyzing applicable insurance coverage.

KEY DEADLINES

Obligation	Deadline
Compliance of AI systems already in use or under development for law enforcement purposes with the provisions of Title I	Within 1 year from the entry into force of the Decree (by September 2027)
Issuance of the ministerial decree establishing technical requirements for real-time remote biometric identification systems	To be determined (Decree of the Minister of the Interior and the Minister of Justice)
Adoption of the Prime Minister's Decree governing regulatory sandboxes	To be determined

Contacts

Turin Corso Vittorio Emanuele II, 68 10121 | T. +39 011 51121

Milan Via Bigli 2, 20121 | T. +39 02 303049

info@pavesioassociati.it – www.pavesioassociati.it

For more information:

AreaLegaltech@pavesioassociati.it

AreaCompliance@pavesioassociati.it

AreaLitigation@pavesioassociati.it

This document is drawn up in general terms, solely for dissemination purposes and regulatory updating.