Italy's AI rules reach the courtroom: litigation tools, corporate risks and judicial function and independence

Italy's latest AI legislation gives claimants new ways to obtain evidence and exposes companies to additional criminal and compliance risks. It also raises a harder question for the courts to address: what happens if AI does more than help write a judgment and actually contributes to shaping the judge's reasoning?+

At a glance. *Italy has strengthened the tools available in disputes over AI-related harm, including access to technical records and a rebuttable presumption of causation in certain cases involving breaches of the EU AI Act. It has also introduced new criminal offences and potential corporate liability. Meanwhile, the courts face an unresolved question: if AI contributes to an assessment that only a judge may make, what happens to the judgment?*

02/11/2026

Roberto A. Jacchia
Alessandro Foti

Italy's AI rules: three measures, different deadlines

The EU AI Act provides the common framework. But anyone advising a business or conducting litigation in Italy also needs to consider the country's own implementing legislation.

Three recent measures deserve particular attention:

- Law No. 132/2025 sets out Italy's general principles for AI, including strict limits on its use in judicial decision-making.
- Legislative Decree No. 160/2026, in force since 30 September 2026, introduces new rules for damages claims and extends certain criminal offences and corporate liability risks.

- Legislative Decree No. 179/2026, in force since 23 October 2026, identifies the supervisory authorities, sets out enforcement powers and sanctions, and provides for regulatory sandboxes (supervised settings in which AI systems can be tested) and training.

The dates need to be read together, not as a single AI Act deadline.

Regulation (EU) 2026/1744 has deferred in time much of the AI Act's framework for high-risk systems. The relevant Chapter III requirements will generally apply from 2 December 2027 to systems covered by Article 6(2) and Annex III (including certain AI tools used in justice), and from 2 August 2028 to systems covered by Article 6(1) and Annex I (AI linked to specified regulated products). Article 6(5) remains subject to a specific exception.

Separate transitional rules apply to certain systems already in use. These changes do not suspend the AI Act as a whole, nor do they affect Article 15 of Italy's AI Law, which reserves judicial decisions to the judge. In any damages claim based on an AI Act breach, the first step is therefore to identify the obligation allegedly breached and check that it applied at the relevant time. A new domestic remedy cannot bring forward an EU obligation that has been deferred.

Civil litigation: how claimants can obtain AI evidence

In AI-related damages litigation, a claimant may have a prima facie claim but little insight into how the system worked. The records are often held by the provider (the organisation developing or placing the system on the market), the deployer (the organisation using it), or another third party. Articles 16(1) and 17 of Decree 160/2026 seek to address that imbalance. In contractual and non-contractual damages proceedings, the court may order disclosure of specifically relevant information where the claimant produces facts and supporting material making the claim plausible, including a plausible connection between the output and the alleged harm. This is a remedy available within proceedings that are pending, not a general right to inspect a system before suing.

The evidence may include system logs (records of the system's activity), risk-management files, technical documents and records of human oversight. Disclosure must be proportionate and protect confidential information and trade secrets. Refusal to comply can have different consequences. Under Article 116 of the Italian Code of Civil Procedure, the court may draw adverse inferences from a party's conduct. Where a party unjustifiably withholds the documents specifically covered by Article 17(2), the court must, after assessing the other evidence, treat the claimant's alleged facts as admitted. A non-compliant third party may instead face a fine of EUR 1,500 to EUR 10,000, which may or may not for practical purposes operate as a deterrent.

Claims based on an applicable AI Act obligation benefit from a further rule. Under Articles 16(2) and 18, the causal connection between the breach and the loss is presumed, subject to proof of the contrary. The wording leaves the true question open: how much evidence of causation must the claimant provide for starters to trigger the presumption? Requiring full proof would defeat the purpose of the presumption mechanism. The rule does not presume that an infringement occurred or that a loss was suffered, and does not make AI providers automatically liable for every harmful output (no strict liability principle) Conversely, Article 19 confirms that compliance with the regulatory framework, even if certified, does not in itself rule out liability.

Article 20 also permits a direct claim against the allegedly responsible party's liability insurer, up to the policy limits. The insurer can invoke contractual defences arising before the loss, and the allegedly responsible party must be joined in the proceedings. The direct claim is subject to the same limitation period as the claim against that party. A claimant may request insurance details, which must be supplied within 30 days,

but need not make that request before issuing proceedings. The decree does not impose compulsory AI insurance or broaden the terms of an existing policy. Separately, Article 16(4) gives consumers an additional choice of court based on where they live or are domiciled.

These rules sit alongside existing routes to compensation, including Article 82 of the General Data Protection Regulation (GDPR) and product liability. The revised EU Product Liability Directive (Directive (EU) 2024/2853) expressly covers software, including AI systems. At the date of writing, the Italian measures implementing that directive were still at the draft stage (Government Act No. 434). Italy must transpose it into national law by 9 December 2026. Under the corrected EU text, its scope concerns products placed on the market or put into service from that date, rather than simply losses occurring afterwards.

Criminal offences and the company's compliance model

The new legislation also matters outside the civil courts, particularly for businesses developing or using high-risk AI.

Article 12 of Decree 160/2026 adds Article 437-bis to the Italian Criminal Code. It targets specified failures to put in place technical safeguards or human oversight (people able to monitor and intervene in a system's operation), as well as certain unlawful changes to high-risk systems, where the conduct creates danger to life, safety or State security identified by the statute. The required state of mind of the wrongdoer differs between offences: the gross-negligence provision applies to conduct under the first paragraph, while a professional user's failure to provide human oversight is punishable only if intentional. An AI compliance shortcoming is therefore not automatically a criminal offence. Equally, deferred EU compliance dates do not per se produce immunity: liability depends on the conduct, the person responsible, the obligation applicable at the relevant time and the danger created.

The decree moreover amends Legislative Decree No. 231/2001, Italy's chief legislation on corporate administrative liability for specified offences committed in an entity's interest or for its benefit. New Article 25-vicies includes Article 437-bis and the unlawful dissemination of certain AI-generated or altered content under Criminal Code Article 612-quater. The respective monetary sanctions range from 600 to 1,000 and from 200 to 700 'quotas' (statutory units used to calculate a company's financial penalty); certain disqualification measures may also apply. A criminal offence does not automatically make the company liable: the statutory attribution rules must still be met. Businesses should review their organisational and compliance model under Decree 231 (commonly called the 'Model 231') and, above all, check whether the controls work in real life: who authorises changes to AI systems, who supervises their operation and how incidents are reported and escalated.

Supervision: who does what in Italy?

Decree 179/2026 allocates responsibility principally between two national agencies. AgID (Agenzia per l'Italia Digitale, Italy's Digital Agency) is the 'notifying authority': it oversees the procedures for designating and monitoring the bodies that assess whether AI systems comply with the rules. Conversely, ACN (Agenzia per la Cybersicurezza Nazionale, Italy's National Cybersecurity Agency) is the principal 'market-surveillance authority', responsible for monitoring compliance and exercising inspection and enforcement powers. Financial regulators and the Italian Data Protection Authority retain their respective roles. The decree also covers penalties, supervised AI testing environments ('regulatory sandboxes') and training, including for the justice system. Although it entered into force on 23 October 2026, not every sanction became applicable on that date; enforcement still depends on when the underlying EU obligation or prohibition takes effect.

For a company operating in Italy, the practical question is not simply whether it

is 'AI Act compliant'. It is which rules apply to its particular system, which regulator oversees its activities and when each obligation becomes enforceable.

When judges use AI: where does assistance become substitution?

A different, and potentially even more critical, issue arises when the user of AI is the judge.

Article 15(1) of Law No. 132/2025 reserves to the judge all decisions about the interpretation and application of law, the assessment of facts and evidence, and the adoption of judicial measures. This provision does not use the word 'delegation'. The real question is whether the judicial assessment was the judge's own, not merely whether the judge signed the finall text. At the same time, considering an AI-generated suggestion is not, by itself, proof that the judicial function was surrendered. Article 15(3) separately makes experimentation and use of AI in ordinary judicial offices subject to Ministry of Justice authorisation under the transitional arrangements.

The Consiglio Superiore della Magistratura (CSM, Italy's High Council for the Judiciary and the judiciary's self-governing body) addressed this boundary in its recommendations last updated on 22 July 2026. The recommendations envisage controlled support, including language editing and structured analysis of case materials, but clearly rule out generating the operative part of a judgment (the section stating the court's order) or entrusting AI with drafting judicial decisions. They also expressly restrict unauthorised tools. Breaching those operational rules is not necessarily the same as unlawfully delegating an assessment under Article 15, and neither automatically establishes that the judgment is void. The CSM recommendations address ordinary judicial offices; whilst Italy's tax courts have a separate institutional framework.

Two recent decisions illustrate why the distinction matters.

In Order No. 182/2026, published on 23 July 2026, the Cagliari Court of Appeal dealt with an application to suspend enforcement of a first-instance judgment while an appeal was pending (Oristano judgment No. 178/2026). A chatbot-style instruction had accidentally been left within the judgment. The appeal court treated it as an indication that AI had assisted with drafting, but not, on its own, as proof that the judge had unduly entrusted interpretation, evaluation or the very decision itself to the system. The court ordered a partial stay for reasons relating to damages, not the AI complaint, and did not decide the merits of the appeal. A similar chatbot artefact was reported in a Palermo first-instance tax judgment (No. 981/2026, Section 11, deposited on 17 February); that incident did not resolve whether AI involvement invalidates a judgment.

What matters is not who typed the words. Asking for a system to improve the style of reasoning already reached by the judge is different from asking it to weigh evidence, choose an interpretation or provide the decisive assessment. But 'influence' alone is too broad a test: submissions from counsel, legal research and precedents routinely influence judges. The issue is whether the judge independently considered and evaluated the relevant materials, or allowed AI instead to carry out part of the assessment that the law reserves to the court.

If AI crosses the line, is the judgment invalid?

Article 15 does not expressly say what happens to a judgment if the statutory boundary is crossed.

The summary analysis that follows concerns civil proceedings; criminal and tax cases have their own rules of challenge.

Some mistakes associated with AI already fit familiar grounds of appeal: made-up precedents, factual findings with no support in the case file, failure to decide a claim, or a statement of reasons that is merely apparent (words are given, but they do not explain the decision).

None follows automatically from finding a chatbot phrase in a judgment. The harder case is a coherent, well-reasoned text where reliable evidence nevertheless shows that an essential assessment came from AI and was adopted without independent judicial scrutiny.

It has been argued that this is a defect in the formation of the judicial decision itself, not simply in its drafting. But Italian civil procedure places limits on how the nullity of a judgment can be established. Article 156 of the Code of Civil Procedure generally requires a statutory basis for nullity arising from a defect of form, while also recognising defects that prevent an act from fulfilling its essential purpose. Treating proven AI substitution as such a defect would, though, require a further interpretative step, as Article 15 does not expressly make the judgment void. In Criminal Cassation judgment No. 34481/2025, the Supreme Court emphasized the judge's indispensable independent evaluation in a case involving reasoning drawn from investigative material. That principle is relevant, but the Court did not rule on an AI-generated judgment or establish a new ground of civil nullity.

A further obstacle comes from the Court of Cassation's Grand Chamber (the Supreme Court in its highest formation for resolving important legal questions of principle). In judgment No. 642/2015, concerning civil and tax proceedings, the Court held that reproducing a party's arguments does not in itself invalidate a judgment if the reasons are clear, complete and capable of sharing by the judge. Judges are not required to write every sentence from scratch. The analogy with AI is imperfect, however: an algorithmic text could introduce facts or authorities that were never part of the case, raising separate concerns about evidence and the parties' opportunity to rebut it. The point remains that an appeal should identify a real defect in judicial evaluation or procedure, rather than rely solely on the origin of the wording.

Legal inexistence (inesistenza giuridica) is a different and much more exceptional case, occurring when the purported judgment is so fundamentally defective that it cannot properly be treated as a judicial act. Under Article 161 of the Code of Civil Procedure, defects in judgments must ordinarily be raised through the available lines of appeal and within the appllicable deadlines; the absence of the judge's signature is an express exception to that rule. Cassation Order No. 9910/2021 deals with this exceptional category and recalls cases where the reasons and operative ruling related to a different dispute entirely. It did not address AI. Arguing that a judgment genuinely issued and signed by the competent judge is legally inexistent because AI was misused would therefore require a much stronger justification than the mere discovery of an AI-generated passage. Nor could such an allegation be assumed to bypass ordinary appeal deadlines.

The remaining challenge: how could it be proved?

The prompts (instructions given to the system), source materials, AI outputs and revision history could help reconstruct what a judge asked the system to do. They would not necessarily show whether the judge later tested the response, discarded parts of it or reached an independent assessment. Obtaining these records would also require a lawful procedural basis. Article 17 of Decree 160/2026 permits targeted disclosure in AI damages claims; it does not create a general right to inspect a judge's deliberations. In practice, the parties are more likely to start with the judgment and the case file, to look for invented citations, factual assertions without evidential support, or overlook objections or reasoning unrelated to the dispute. These may justify further scrutiny provided the available tools are still capable of resort, but do not automatically prove unlawful delegation of the jurisdictional function to a machine.

For businesses, the immediate task is to understand what records their AI systems generate, preserve relevant evidence where a dispute is reasonably anticipated and document how human oversight works in practice, while respecting confidentiality and data-protection requirements. For litigators,

the stronger approach is to identify the assessment allegedly made by AI, explain why it mattered to the outcome and connect it to a recognised ground of appeal within the applicable time limits. In the end, the central question is not whether AI helped produce the words of the judgment, but whether the judgment itself remained the judge's own.

Selected sources

EU AI Act (Regulation (EU) 2024/1689) | Regulation (EU) 2026/1744 | Italian Law No. 132/2025, Article 15

Legislative Decree No. 160/2026, Articles 12 and 15–20 | Legislative Decree No. 179/2026 | CSM recommendations, update of 22 July 2026, reproduced text

Product Liability Directive (EU) 2024/2853 | Corrigendum of 7 May 2026, Article 2(1) | Chamber of Deputies, Government Act No. 434.

Code of Civil Procedure, Article 156.



Roberto A. Jacchia
PARTNER

r.jacchia@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano



Alessandro Foti
MANAGING ASSOCIATE

a.foti@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com