

COMPLIANCE & GOVERNANCE

DEEPFAKES AND IMPERSONATION

*WHEN **OUT-OF-COURT REMEDIES** ARE NOT
ENOUGH: **JUDICIAL PROTECTION OF THE
COMPANY***

AUTORI

Avv. **MAURIZIO MARULLO**
marullo@lawp.it

Avv.st. **ALESSANDRA MOSCA**
mosca@lawp.it

In our previous contribution, we examined how the response to an attack involving deepfakes or impersonation cannot rely solely on technical tools: preserving evidence, taking action against platforms, blocking financial transactions, and coordinating across corporate functions are the first lines of defence.

But what happens when these measures are not sufficient?

A manipulated video may continue to circulate despite removal requests; a fake account may continue to publish content attributed to senior company executives; a cloned voice may already have resulted in a payment being made. In such cases, incident management moves into the phase of judicial protection.

The issue is particularly timely. **Legislative Decree No. 160 of 9 September 2026**, published in the Official Gazette on 15 September 2026 and effective as of 30 September 2026, introduces civil procedural mechanisms for actions seeking compensation for damage caused through the use of artificial intelligence systems.

1. STOPPING THE ATTACK: URGENT INTERIM RELIEF

Where the damage is still ongoing, waiting for the outcome of ordinary proceedings may render judicial protection essentially ineffective. This may occur, for example, where a deepfake attributed to the Chief Executive Officer continues to be shared on social media, or where false communications are disseminated through accounts impersonating the company's official accounts.

Where the relevant requirements are met, an **application for urgent relief pursuant to article 700 of the Italian Code of Civil Procedure** may be relevant, enabling the applicant to request that the court order measures capable of preventing the time required for ordinary proceedings from causing imminent and irreparable harm.

The claim must be tailored to the specific circumstances of the case. For example, it can be request the cessation of the dissemination of certain content, its removal, or an injunction against further publication. URLs, accounts, posts, videos, and methods of dissemination must be identified and documented where possible.

Where the relevant requirements are met, the interim measure may be accompanied by the application of **article 614-bis c.p.c.**, providing for a sum to be payable for each subsequent violation or delay in compliance. This is particularly useful where the content continues to be republished.

On the issue of continued online availability and de-indexing, see Italian Supreme Court, Civil Division I, No. 14488/2025.

2. ONCE THE ORDER HAS BEEN OBTAINED, IT MUST BE EFFECTIVELY ENFORCED

In particularly urgent cases, where prior notice to the opposing party could jeopardise the implementation of the measure, the court may issue an order *inaudita altera parte* pursuant to Article 669-sexies c.p.c.

A provisional decree is thus issued and a hearing is scheduled for the parties to be heard. The applicant must serve the application and the order within the time limit prescribed; following the hearing, the measure may be confirmed, amended or revoked.

For the company, obtaining the order means ensuring its proper service, monitoring compliance with it, and documenting any further publications or infringements.

In relation to obligations to do or refrain from doing an act, article **669-duodecies of the Italian Code of Civil Procedure** empowers the Court that granted the interim relief to oversee its implementation and resolve any difficulties arising in the course of enforcement.

3. WHAT IF WE DO NOT KNOW WHO THE PERPETRATOR IS?

One of the most frequent problems in deepfake and impersonation attacks is anonymity: the company may be aware of the unlawful content, the account and the platform used, but not the identity of the person operating that account.

Identifying the individual against whom proceedings should be brought may require coordination between civil proceedings, the competent authorities and the relevant intermediaries.

The Digital Services Act is also relevant in this context: articles 9 and 10 govern orders addressed to intermediaries to counter specific instances of illegal content and to obtain information concerning specific recipients of their services.

In parallel: reporting the matter to the authorities

Alongside civil remedies, where the facts may constitute a criminal offence, the company may consider filing a criminal report or, where required, a formal criminal complaint (querela), including with the Postal and Cybersecurity Police (*Polizia Postale*).

Criminal proceedings are particularly relevant where the perpetrator has not been identified, as investigative activities may obtain data relating to accounts, IP addresses, devices and other evidence that is not available to the company.

A criminal report or complaint may be filed with judicial police offices or with the competent judicial authority; the appropriate course of action depends on the offence in question and on the applicable procedural requirements.

The Online Public Security Police Station (*Commissariato di P.S. online*) enables reports to be submitted and assistance to be requested from the Postal and Communications Police, but does not replace, where required, a formal criminal report or complaint.

Criminal proceedings do not replace civil remedies: the two avenues may be pursued in parallel and serve different purposes, namely the investigation and establishment of the offence and of criminal liability, on the one hand, and the cessation of the unlawful conduct, protection of the rights infringed and recovery of damages, on the other.

4. FROM 30 SEPTEMBER, THE ISSUE OF EVIDENCE WILL CHANGE

ABOVE ALL

Legislative Decree No. 160/2026 introduces a dedicated Chapter on “civil procedural mechanisms for the recovery of damages caused by the use of artificial intelligence systems”, applicable to both contractual and non-contractual claims for damages.

Article 17 allows a person alleging that they have suffered damage to apply to the court for an order requiring the opposing party, or any third party in possession or control of the relevant evidence, to disclose relevant evidence concerning the operation of the system, provided that the applicant submits sufficient elements to make the merits of the claim and the causal link between the system's output and the damage suffered plausible.

The evidence referred to includes system logs, risk-management and technical documentation, system parameters and records of human oversight. Any such order must be necessary and proportionate and must ensure the protection of confidential information.

Where a party fails to comply with the order without justified cause, the court, having regard to all other available evidence, may deem the facts alleged by the applicant to have been established. In the event of non-compliance by a third party, a pecuniary penalty ranging from EUR 1,500 to EUR 10,000 may be imposed.

5. CAUSATION WILL NOT ALWAYS HAVE TO BE ESTABLISHED ENTIRELY BY THE INJURED PARTY

Article 18 of Legislative Decree No. 160/2026 provides that, where the damage results from a breach of obligations laid down by the AI Act, the causal link between the breach and the damage is presumed, unless proven otherwise.

This provision is particularly relevant in proceedings characterised by a significant information asymmetry.

Articles 18 and 19 do not apply to every dispute involving an AI system, but only where the damage results from a breach of obligations under the AI Act, for example in relation to risk management, technical documentation or human oversight. **Article 19** further clarifies that the system's compliance, even where certified, does not in itself exclude the defendant's liability.

This distinction is also important in the context of deepfakes. If a fraudster uses voice-cloning software to impersonate the CFO and induce an employee to arrange a bank transfer, AI may simply be the instrument used to perpetrate the fraud. Its use does not automatically trigger the application of articles 18 and 19: it must be determined whether the damage resulted from a breach of an obligation under the AI Act. Otherwise, the ordinary rules of civil law governing liability, causation and evidence apply.

In such cases, the principles developed by the Italian Supreme Court in relation to phishing and fraudulent payments are relevant (Italian Supreme Court, Civil Division III, No. 3780/2024).

6. BEING "AI ACT COMPLIANT" DOES NOT AUTOMATICALLY CLOSE THE ISSUE

For companies, documenting compliance remains essential, however certification does not, in itself, constitute an exemption from liability.

Article 20 allows a person intending to bring a claim for damages to ask the party whom they consider responsible for the damage whether that party is covered by civil liability insurance. Within thirty days, the relevant party must provide details of the insurance coverage, the policy and the insurer.

Subject to the policy limit, the injured party has a direct right of action against the insurer, without prejudice to the mandatory joinder of the party identified as liable.

7. FROM INCIDENT MANAGEMENT TO LITIGATION STRATEGY

The new decree does not replace the remedies already available. If a deepfake continues to circulate, the priority may be to obtain an interim order promptly; if the responsible party has not been identified, it will be necessary to address attribution and obtain the information required to identify the perpetrator; if damage has already occurred and the issue of compensation arises, from 30 September the mechanisms introduced by Legislative Decree No. 160/2026 may have their greatest impact in the evidentiary sphere.

The distinction is between two complementary needs:

- **stopping the damage**, through the interim remedies already available under the Italian law;
- **proving and obtaining compensation for the damage**, including through the new procedural mechanisms introduced for artificial intelligence systems.

The new decree does not remove litigation concerning AI systems from the scope of the ordinary rules of civil law. Rather, it introduces mechanisms designed to reduce information asymmetry in establishing how the system operates, the causal link and liability.

For companies, responding to a deepfake or impersonation attack does not end with identifying and containing the incident. Where an out-of-court response is insufficient, it is essential to determine what relief to seek from the court, against whom proceedings should be brought, and what evidentiary material should be obtained.