

COMPLIANCE & GOVERNANCE

DEEPFAKE AND IMPERSONATION

*WHY PROTECTING THE COMPANY IS NOT JUST AN
IT ISSUE, BUT A **LEGAL AND GOVERNANCE
STRATEGY***

AUTORI

Avv. [Maurizio Marullo](#)
marullo@lawp.it

Avv. [Claudia Marongiu](#)
marongiu@lawp.it

1. INTRODUCTION

In July 2024, a Ferrari executive received several WhatsApp messages apparently sent by the Company's Chief Executive Officer. Shortly afterward, he received a phone call: on the other end of the line, a voice reproduced using deepfake techniques, so realistic that it was difficult to detect the deception from listening alone, told him that action was required in connection with a financial transaction. The attempted fraud was thwarted not by an IT safeguard, but by the executive's alertness: faced with a voice identical to that of the Chief Executive Officer, he sought confirmation by asking a question about a book that had been recommended to him privately, forcing the fraudster to hang up without answering.

The incident highlights a risk scenario companies must necessarily face: generative AI techniques can accurately reproduce the physical features, tone of voice and communication style of senior executives, meaning that **voice, image and video can no longer, by themselves, be regarded as sufficient elements for verifying the communicator's identity.**

2. BEYOND CYBER FRAUD: THE IMPACT OF DEEPPAKES ON COMPANIES

Deepfakes and impersonation carried out using artificial intelligence tools are not simply cyberattacks, but advanced manipulation tools used to:

- induce unauthorized payments or changes to bank account details (so-called *CEO fraud*);
- steal credentials, confidential information or trade secrets;
- circulate false statements or instructions attributed to senior management.

Consequently, the potential damage caused by these tools extends beyond the technological sphere, affecting the company's financial stability, business continuity, compliance and market reputation.

3. FROM PREVENTION TO MANAGEMENT: BUILDING THE RESPONSE BEFORE AN ATTACK

Relying solely on an individual employee's intuition or alertness to detect a deepfake-based fraud attempt exposes the company to excessive risk. An effective defense must be based on a **comprehensive strategy, structured in at least three phases:**

Phase 1: Prevention and risk management

Technical measures alone are not sufficient to mitigate the risks associated with deepfake-based attacks. They should be complemented by a proactive assessment of the main risk scenarios, with the findings translated into appropriate organizational safeguards and procedures. This requires coordinated collaboration between IT/cybersecurity, compliance, legal, and finance teams. In particular, organizations should:

- **identify the most exposed processes**, such as payment authorization, changes to suppliers' bank details, or the handling of confidential information;
- **establish identity-verification procedures using independent channels already known to the organization**, especially for more sensitive or unusual requests;
- **establish clear reporting and escalation procedures**, so that personnel know whom to contact and which steps to activate in the event of unusual or suspicious requests, communications or conduct.

Phase 2: Incident management and immediate measures

As soon as an anomaly is detected, it is essential to promptly activate the competent corporate functions and ensure their coordination, involving, depending on the nature of the incident, the IT/cybersecurity, compliance, legal, finance and communications functions.

The initial response must pursue two parallel objectives: **contain the effects of the attack and preserve the elements needed for subsequent legal protection measures**. Before deleting messages, removing content or disabling accounts, it is therefore advisable to preserve original files, URLs, messages, the accounts used, dates and times of communications, screenshots, any metadata, and any other information useful for documenting how the attack was carried out and how it spread.

At the same time, any **available out-of-court containment measures** should be activated. Depending on the nature of the attack, this may involve immediately contacting banks or payment service providers to attempt to block or recall a fraudulent transaction; reporting fake or compromised accounts to the relevant platforms; submitting requests for the removal or disabling of manipulated content; and, where necessary, issuing communications to customers, employees, suppliers or other persons potentially exposed to the fraud.

Speed of intervention is essential, but it must not result in isolated actions. Technical, financial, legal and communications measures must be coordinated, because an intervention aimed at containing the attack may affect the preservation of evidence and the company's subsequent avenues for legal protection.

Phase 3: Recovery, out-of-court protection, compliance obligations and assessment of liability (after the attack)

Once the first containment measures have been adopted, the response must continue on both the technical and the legal and regulatory fronts.

From a legal perspective, at this stage it is first necessary to reconstruct what happened and consolidate the documentation collected, so as to have the elements needed to assess any further action to be taken.

Depending on the characteristics of the incident, **further out-of-court measures** may be necessary, such as sending cease-and-desist letters and formal requests to stop the conduct or remove the content (where the perpetrator of the fraudulent conduct is known or, alternatively, has been identified with the assistance of the competent bodies entrusted with that task, such as the Postal and Communications Police), engaging with digital platforms, providers and other intermediaries involved, and taking the steps necessary to counter the spread of communications falsely attributed to the company or its representatives.

It must also be determined whether the attack resulted in an **incident relevant to the notification obligations under Legislative Decree No. 138 of 4 September 2024, implementing Directive (EU) 2022/2555 (NIS2)**, or in a **personal data breach within the meaning of Regulation (EU) 2016/679 (GDPR)**, with the resulting need to assess any obligations to notify the supervisory authority and, where the relevant conditions are met, to communicate the breach to data subjects pursuant to Articles 33 and 34 GDPR. The potential applicability of any additional communication or notification obligations under sector-specific legislation must also be assessed.

Where the relevant conditions are met, it will also be necessary to assess whether to file complaints or reports with the competent authorities. At the same time, possible grounds of liability will need to be identified and the effectiveness of the out-of-court measures already taken assessed.

4. THE ADDED VALUE OF LEGAL SUPPORT: FROM A REACTIVE FUNCTION TO ONE OF PREVENTION AND PROTECTION

Traditionally, the in-house or external legal team tends to be involved mainly after a cyberattack has occurred, when it is necessary to file a complaint, request the removal of content, send a cease-and-desist letter, or assess whether to commence legal proceedings.

In the face of deepfake-based threats, however, a purely reactive approach is no longer sufficient. The legal function's contribution becomes important already at the prevention stage, in coordination with the technical, finance and compliance functions, so that the measures adopted by the company take into account, from the outset, the possible legal and regulatory implications.

Early involvement of the legal team makes it possible, in particular, to verify that internal procedures are consistent with the applicable regulatory framework; contribute to defining roles, responsibilities and decision-making processes in the event of an incident and identify in advance the elements that will need to be preserved and the assessments to be made if communication or notification obligations arise. It also makes it possible to incorporate the risk of deepfake and impersonation attacks into the company's broader governance and risk-management system, including with regard to organizational arrangements and the responsibilities of corporate bodies.

The value of legal expertise, therefore, is not limited to the possible commencement of court proceedings. Its contribution is essential even before an incident occurs, in defining prevention and response procedures, and in the early stages after an attack, when it is necessary to preserve evidence, coordinate containment measures, activate out-of-court remedies, and assess any communication or notification obligations.

When these tools prove insufficient, the issue of judicial protection for the company arises. The next contribution will be devoted to this further level of response, and, in particular, to the actions that may be brought before the courts following a deepfake or impersonation attack.