

Boardroom liability: protecting advice, governing AI

At the IBA conference in Copenhagen, white-collar crime specialists examine the limits of legal privilege across European jurisdictions and what boards need to understand about AI-related risks

by flavio caci

COPENHAGEN — Boards need legal advice before problems become criminal investigations. They also need to understand which communications will remain protected if prosecutors intervene. As companies adopt AI, a further question arises: what must directors know, oversee and document to demonstrate that they are managing the risks? These issues emerged from discussions at the International Bar Association's annual conference in Copenhagen. *MAG* attended the session on "*Criminal law in the boardroom*" and spoke with white-collar crime specialists from Germany, Italy, Spain and Switzerland about the implications for directors and their advisers.

LEGAL PRIVILEGE: KNOWING THE LIMITS

The scope of protection for lawyer-client communications varies between jurisdictions. For directors and advisers working across borders, assumptions formed in one legal system may not hold in another.



CONSTANTIN LAUTERWEIN



ANDREA PUCCIO

Constantin Lauterwein, a white-collar partner at Hengeler Mueller's Berlin office, points to a structural difference: "We don't have the same concept of privilege of the United States or the UK". In his account of the German position, the distinction between general board advice and communications connected to a criminal defence is central. For corporate lawyers, Lauterwein says, the result is a constant balancing act between protecting the company and meeting documentation obligations.

Along the same line **Andrea Puccio**, founder of Puccio Penalisti Associati, highlights the importance of the defence mandate in Italy, where "legal privilege doesn't exist, unless an external counsel is appointed in a criminal investigation, for a criminal defense". The practical consequence, he says, is that lawyers learn to be careful about what they put in writing, even though some foreign clients ask for written reports.

Simone Nadelhofer, a partner at Schellenberg Wittmer in Zurich, adds a further complication.

In Switzerland, she notes, privilege extends only to communications with externally admitted lawyers acting in a conventional legal capacity. She cautions that material produced by an in-house legal team, or generated by AI, should not be assumed to be protected from prosecutors in criminal proceedings.

INVESTIGATIONS: TIMING AND THE COUNSEL'S MANDATE

For Nadelhofer, timing matters. External counsel should be brought in as soon as proceedings become reasonably foreseeable. She emphasises preserving data and escalating the matter internally at the initial stage.
The mandate should be structured, and documented, as legal advice in view of potential proceedings or criminal defence. Ideally, she says, the board rather than management should instruct counsel, particularly where the stakes are high or management is itself a cause for concern.



SIMONE NADELHOFER

Nadelhofer points to Swiss cases in which courts denied protection to banks whose purported investigations were, in substance, outsourced compliance work. And because the window for asserting privilege over seized documents is short, external counsel must be ready to claim it at once.
The difficulty compounds when several jurisdictions investigate the same facts at the same time, she notes. Material that is protected, or even required, in one country may be unprotected, or prohibited outright, in another. In Switzerland, she says, handing evidence directly to a foreign authority can itself breach the criminal code, while secrecy and data-protection rules constrain cross-border transfers. Expectations of cooperation, and the rights of the individuals involved, diverge further still, notably between the US and Switzerland.

AI: REGULATORY DUTIES AND CRIMINAL EXPOSURE

In Copenhagen, on the panel's sidelines alongside the question of how legal advice is protected comes that of how boards discharge their responsibilities as technology changes. Here, the lawyers distinguish between new regulatory requirements and the conditions for personal criminal liability.
Juan Palomino, a partner at Pérez-Llorca in Madrid, says that what European AI regulation changes "is not so much the source of liability, as the standard against which boards will be judged". Until recently, he explains, AI could comfortably be treated as a technology issue and delegated to specialists. That is getting harder, as "under the emerging EU framework, boards are expected to demonstrate that AI-related risks are being identified, understood and governed in the same way as cybersecurity, financial reporting or regulatory compliance".
For Andrea Puccio, who works in a European and Italian regulatory landscape that has added new categories of offence and widened corporate liability, the main challenge as a criminal lawyer "will be to avoid automatic attributions of criminal liability to members of the board of directors, especially in a sector where technology



ELISEO M. MARTÍNEZ

evolves faster than the rules".

Eliseo M. Martinez, managing partner at the Madrid-based Ius+Aequitas, says his main concern is "that companies may adopt AI faster than they update their internal controls." Spain introduced corporate criminal liability in 2010, and AI adds a new dimension to that framework, he says. Depending on how it is used, it can facilitate fraud, the unlawful disclosure of trade secrets or intellectual-property offences. "Yet," he points out, "neither adopting AI nor breaching a regulatory obligation automatically makes a director criminally liable per se".

BOARD OVERSIGHT: EXPERTISE, CONTROLS AND ACCOUNTABILITY

Martinez says the priority for boards is to revisit their compliance programmes. Companies, in his view, should identify how each use of AI changes their exposure, update their risk assessments, and introduce appropriate protocols, responsibilities, training and oversight. A generic AI policy will not address the different risks that arise in different businesses.

Directors, Puccio adds, "do not need to become technology experts, but they must be able to understand the risks and recognize when to intervene". For businesses, he says, the priority is to move from adopting AI to managing its risks. That requires clear accountability, effective controls, adequate information flows and, above all, ongoing training.

Palomino draws the distinction between technical expertise and board oversight: "directors are not expected to become engineers, data scientists or model developers. What they are expected to do is understand the business implications of AI, recognise when significant risks arise, ensure that relevant expertise exists within the organisation, and challenge management when assurances are insufficient".

Copyright © 2026, LegalcommunityCH



JUAN PALOMINO