CMS | Navigating criminal liability risks for generative AI companies

AI generative technology has revolutionised industries, advancing content creation, automation, and innovation, but its rapid adoption introduces criminal liability risks for developers, providers, and users. For generative AI (*gen-AI*) companies operating in Romania and across multiple jurisdictions, understanding and mitigating these risks is crucial for avoiding legal exposure and fostering trust.

The following article highlights key criminal liability implications surrounding gen-AI in Romania and suggests strategies to ensure compliance and risk mitigation.

Key areas of criminal liability for gen-AI companies

Gen-AI tools, such as content creation platforms, can inadvertently facilitate illegal activities, raising concerns about corporate and individual criminal liability under Romanian and EU law. These risks include content-related offenses, cybercrime (e.g. cybersecurity breaches), intellectual property violations and data privacy breaches.

Gen-AI content and tools may be misused to create the following material that violates the Romanian Criminal Code:

- Child exploitation material or unlawful pornography;
- Incitement to violence, hate speech, or extremist propaganda;
- Defamatory content or fake news;
- Phishing emails, deepfake videos, or malicious software;
- Fake identities or forged documents;
- Automated financial fraud schemes.

Conducting rigorous risk assessments and implementing safeguards can significantly reduce misuse potential.

Jurisdictional challenges in criminal enforcement

Gen-AI companies operate globally, but laws governing AI-related criminal activities vary across jurisdictions, creating the following challenges, among others:

→ Jurisdictional conflicts: An AI tool may violate laws in one country while remaining compliant in another.
→ Extraterritorial reach: Increasingly, countries are enforcing criminal laws extraterritorially to address cross-border cybercrime and content offenses (e.g. EU's Digital Services Act, US federal cybercrime laws).

→ Regulatory uncertainty: Rapid AI adoption outpaces legislative developments, leaving room for ambiguity regarding potential criminal liability.

The Digital Services Act (**DSA**) introduces "safe harbour" rules that provide liability exemptions for intermediaries, provided they act expeditiously to remove or disable access to illegal content upon learning of its existence. These provisions highlight the importance of maintaining transparent content moderation systems and responding swiftly to flagged violations.

Legal professionals specialising in multi-jurisdictional compliance may assist in aligning operations with applicable laws and regulations.

Corporate criminal liability for Gen-AI companies

In almost all jurisdictions, companies can be held criminally liable for offences committed through their platforms or by their representatives/employees if:

→ they fail to implement adequate measures to prevent illegal activities (e.g. lack of content moderation); senior management knowingly permits or ignores unlawful use of their technology.

Romanian law recognises corporate liability under Article 135 of the Criminal Code if offences occur during business operations. Companies may face charges for:

→ Negligence and recklessness: Failing to supervise AI systems that generate illegal content or facilitate crimes.
→ Complicity: Enabling or aiding criminal activities committed by end-users through the misuse of their tools, through insufficient oversight or deliberate inaction.

Recent allegations against a major social media platform for allowing its livestreaming feature to facilitate child exploitation demonstrate the severe consequences when systems are not monitored adequately. Such examples highlight the necessity for companies to prioritise robust oversight mechanisms and actively address risks associated with their technology.

To address these risks, companies should establish governance frameworks with clear accountability structures, adopt robust content moderation systems, and provide targeted training to senior management to ensure awareness of potential liabilities.

Conclusion

Gen-AI companies must navigate ever-evolving criminal liability risks by understanding their exposure, implementing safeguards, and collaborating with specialised legal counsels. Proactive compliance protects against legal repercussions while fostering trust and innovation. Legal experts play a critical role in identifying jurisdiction-specific obligations, crafting effective mitigation strategies, and providing representation during investigations or litigation. Obtaining guidance from professionals who are experienced in international criminal law and AI regulations ensures that a company’s compliance measures will be robust and practical, and will enable the company to mitigate future risks effectively while maintaining operational integrity and global competitiveness.

For more information on the risks of generative AI and how to mitigate these risks, contact your CMS client partner or these CMS experts: **Mihai Jiganie-Serban** and **Anca Elena Toma**.