MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Open Access Journal of Criminology Investigation & Justice
ISSN: 3064-7940

Corporate Criminal Liability and Artificial Intelligence: Doctrinal Overview, Problems and Perspectives

Cutolo M*

Ph.D., LL.M., Visiting Researcher, USA

***Corresponding author:** Mattia Cutolo, Ph.D., University of Salerno Law School (IT), LL.M. Washington University School of Law (USA), Visiting Researcher University of Pennsylvania Carey Law School (USA), Tel: (+39) 340-512-2794; Email: mcutolo@unisa.it

Short Communication
Volume 2 Issue 1
Received Date: September 10, 2024
Published Date: October 15, 2024
DOI: 10.23880/oajcij-16000122

Abstract

Integrating artificial intelligence (AI) in corporate strategies introduces significant challenges to corporate criminal liability. Traditionally, corporations can be held liable for crimes committed by human agents under the doctrine of respondeat superior, but AI systems complicates this framework. The article explores some legal implications of AI-induced crimes, focusing on the need for robust compliance and risk management practices. It emphasizes the potential for AI to influence corporate decision-making and the conditions under which companies may be held liable for AI-related offenses. The discussion highlights the importance of preventive measures to mitigate these risks and offers insights for stakeholders on navigating the evolving criminal law landscape.

Keywords: AI Corporate Liability; Compliance Risks; AI-Caused Crimes; AI Regulation; Respondeat Superior (principle of)

Abbreviations

AI: Integrating Artificial Intelligence.

Introduction

It is known that corporations may be found criminally liable under the doctrine of respondeat superior if a human agent commits a crime, both in the U.S. [1] and in the E.U. [2]. That is why the adoption of artificial intelligence (AI) in economic and corporate strategies raises novel questions regarding legal implications in terms of AI-related criminal liability, directing attention towards the importance of compliance and corporate criminal liability [3-5].

In an increasingly digitalized world, where AI assumes critical roles in business enterprises, the risk of engaging in unlawful or even criminal conduct due to automated systems becomes a reality that cannot be ignored. Understanding how corporate criminal liability adapts to these new challenges is therefore imperative for companies aiming to integrate AI into their business operations, in a financially fruitful manner without incurring unforeseeable criminal liabilities. This article highlights the general issues of corporate criminal liability concerning the use of AI, analyzing how AI can impact corporate management practices and on what basis companies can be held criminally liable for crimes caused by AI.

It will also discuss how risk prevention and mitigation play a crucial role in limiting the possibility that AI leads to criminal violations committed by agents which trigger corporate criminal liability, presenting tools and strategies that companies can adopt to remain compliant with regulations. This broad analysis aims to provide legislators, legal practitioners, and corporate executives with a general overview on the inferred problematics, navigating the complexity of AI-related liability, promoting greater awareness of the legal implications and necessary compliance measures.

Scientific Interest and Social Context

Corporate criminal liability determines to what extent a company, as a legal entity, can be held accountable for the acts and omissions of its agents or employees acting in the interest or for the benefit of the company. The principles of liability for legal entities help clarify when a legal entity can be held responsible for wrongful acts. These standards vary significantly depending on different legal traditions; for instance, while Australia and Canada anchor their corporate liability systems in criminal law, the German and Italian systems are based on administrative law.

Current regulations reflect a growing interest in AI regulation, underscoring the need for companies to implement usage, privacy, and communication policies. More than half of law firms and 43% of corporate legal departments believe regulations are necessary to govern AI's professional ethics at an industrial level. Furthermore, 66% of professionals believe AI will bring new challenges, primarily related to data accuracy and security. Consequently, human intervention remains crucial to verify the accuracy and reliability of AI output, especially in sensitive or high stakes matters [6].

These principles and regulations are essential to ensure that the adoption and implementation of AI in companies occur responsibly and in compliance with existing laws, promoting ethical practices and reducing the risk of legal liability. Modern corporate management is undergoing a significant transformation thanks to the use of AI and these few paragraphs examine both the benefits and risks associated with the use of AI in business operations.

The adoption of AI in corporate contexts offers numerous advantages, including increased operational efficiency and improved customer experience. According to the "Global State of AI (2022)" report by Frost & Sullivan, 87% of organizations believe that AI and machine learning will help increase revenues, improve operational efficiency, and enhance customer experience [7].

AI thus allows companies to make more accurate decisions, overcoming the limitations of personal intuition, which can be though influenced by biases. Additionally, AI's ability to handle tasks at a volume and speed that exceed human capabilities enables organizations to significantly accelerate business cycles, reducing the time required to go from design to market, thereby improving the return on investment.

Compliance Risks and AI-Committed Crimes

Despite the renown benefits, implementing AI also involves significant compliance risks. Companies must address challenges related to data security and privacy, which require careful management to avoid violations. A McKinsey survey highlights the growing importance of maintaining high standards of data privacy and security in the context of AI, promoting the use of advanced techniques such as homomorphic encryption to protect sensitive information [8].

Moreover, the need for human oversight to interpret AI-generated results is crucial to prevent the reproduction of existing biases, as demonstrated by a Carnegie Mellon University study on Google's online advertising algorithms [9].

The expansion of such field in the legal landscape presents new challenges for law enforcement as well, especially regarding AI-caused crimes [10]. In June, U.S. Deputy Attorney General Lisa Monaco emphasized the importance of vigorous legal action against crimes involving or facilitated by AI, announcing that the U.S. Department of Justice (DOJ) will seek harsher penalties in cases where AI misuse increases the threat of misconduct [11].

This stance has been reiterated in various conferences, highlighting a significant shift in the legal perception and treatment of AI. As a matter of fact, recently the Biden administration issued an executive order on safe, secure, and reliable AI, urging federal agencies to establish standards and guidelines to mitigate AI-related risks [12]. This includes principles of safety, privacy, fairness, and civil rights, consumer protection, support for American workers, promotion of innovation and competition, and collaboration with international partners. The E.U. pays a great deal of attention to such topics as well, as the "AI Act" covers the most important aspects of the AI usage [13].

Despite existing guidelines and regulations, enforcing the law in cases of AI-induced crimes remains complex. Law enforcement authorities face significant challenges in investigating AI misuse, especially when legal violations stem from decisions made by AI systems rather than intentional human actions: in fact, the "AI misuse" refers to both AI affected by programming mistakes and to sel-learning AI which are unpredictable by design. This is further complicated by the rapid evolution of AI technology, which often outpaces current regulatory capabilities.

A significant example of this challenge is the management of so-called "hard AI crimes," where AI agents can commit acts that would be considered crimes if perpetrated by humans, without a clearly responsible human subject. This creates a gap in criminal liability, as neither the AI agent nor the humans behind it can be effectively punished under existing laws. In response, some scholars suggest shifting the focus from culpability to deterrence, proposing an AI deterrence paradigm separate from traditional criminal law [14].

Conclusion

In the corporate context, adopting an AI governance program based on a risk management framework is today more and more common, while the AI usage is alreafy essential to lots of businesses. Organizations and governments are creating and publishing best practices for assessing risks arising from AI development and use as to its compliance risks. Legislative proposals adopt a risk-based approach, requiring companies using "high-risk" AI to comply with additional obligations [15].

Companies must consider implementing security measures to prevent AI misuse by malicious agents or, in general, actors who could introduce malware as to informatic offenses, or poison the AI model with incorrect data as to economic offenses, or not respect rules of conduct as to AI-devices causing physical harm, as to individual safety offenses.

In other words, the most delicate and complex issue is the commission of crimes directly by a self-learning AI in its complete unpredictability by design, such as unauthorized computer access or data theft, or economic crimes in the case of devices programmed for investments (which also pose problems related to money laundering offenses), or as personal injuries in the case of medical devices.

Additionally, it is crucial to establish a well-defined and integrated process for the data, a model and software lifecycle, including standardized processes for development and monitoring, with specific checkpoints where approvals and reviews are necessary. It is clear this process should connect to existing data and privacy governance mechanisms as well as the software development lifecycle.

De lege ferenda, an organization and control model could be established whereby boards of directors control, through periodic reviews, AI systems, especially if used in more sensitive sectors such as telemedicine companies or investment banks.

In this way a corporate criminal model could be created, specifically intended for AI-induced or caused crimes.

Thus, the interest in research aims at exploring the interference profiles between corporate criminal liability and crimes caused or contributed to by AI-equipped devices is evident. This analysis merely consists of a starting point, shedding some light on what types of crimes could trigger corporate liability under the current legal framework in the E.U. and in the U.S., and helping devise new compliance models tailored to the specific risks arising from AI.

References

1. Melissa K, Lee P (2008) Corporate Criminal Liability, in American Criminal Law Review 45(2): 275-303.
2. Gobert J, Pascal A (2011) European Developments in Corporate Criminal Liability, Routledge.
3. Mazzacuva F (2023) The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Holistic Theories, in Revue Internationale De Droit Penal 1: 143.
4. Mongillo V (2023) Corporate Criminal Liability for AI Related Crimes: Possible Legal Techniques and Obstacles, In: Picotti L, Panattoni B (Eds.), Traditional Criminal Law Categories and AI: Crisis or Palingenesis?, in RIDP-International Review of Penal Law 1: 77.
5. Martini G (2023) The Italian Response to Corporate Criminal Liability: a new challenge for artificial intelligence, in European Journal of Privacy Law & Technologies 1: 100.
6. Navigate ethical and regulatory issues of using AI.
7. 12 key benefits of AI for business.
8. 5 AI Risks for Organizations & How Business Leaders Can Overcome Them.
9. AI is having a significant impact on the business world, affecting jobs, workers, firms, and industries.
10. Vattiata LA (2023) AI Systems Involved in Harmful Events: Liable Persons or Mere Instruments? An Interdisciplinary and Comparative Analysis. BioLaw Journal 1: 485.
11. https://www.justice.gov/opa/pr/update-deputy-attorney-general-lisa-monacos-justice-ai-convenings.

12. https://www.sidley.com/en/insights/newsupdates/2024/02/us-department-of-justice-signals-tougher-enforcement-against-artificial-intelligence-crimes.

13. https://artificialintelligenceact.eu/

14. Nerantzi E, Sartor G (2024) ‘Hard AI Crime’: The Deterrence Turn. Oxford Journal of Legal Studies 44(3): 673-701.

15. Solution for mitigating AI risks: meaningful governance.