Chapter 5
The Rise of Deepfake Fraud: Legal Challenges and AI-Driven Detection Strategies

Kaveri Sharma
https://orcid.org/0000-0001-7957-2252
Turon University, Karshi, Uzbekistan

Yunfei Li
Department of Business Sciences, University Giustino Fortunato, Benevento, Italy

Ubaldo Comite
Faculty of Economy, Department of Business Sciences, University of Calabria, Italy

ABSTRACT

Deepfake technology, enabled by advanced AI models like GANs and diffusion networks, has created a new frontier of digital fraud. Its misuse spans financial scams, executive impersonation, political disinformation, and reputational sabotage, producing media nearly indistinguishable from reality. Legal systems remain fragmented and reactive, with inconsistent definitions, weak penalties, and difficulties in establishing liability among creators, platforms, and AI developers. The global spread of deepfakes

DOI: 10.4018/979-8-3373-5992-2.ch005

complicates enforcement, while regulators must balance intervention with freedom of expression. This paper analyzes comparative legal responses in the European Union, United States, India, and China, alongside technological defenses such as AI classifiers, blockchain verification, and biometric tools. It advocates for harmonized laws, stronger detection, and corporate accountability to confront evolving risks.

1. INTRODUCTION

1.1 The Emergence of Deep-Fake Technology

The advent of deepfake technology represents one of the most consequential disruptions in the digital era. Deepfakes, short for "deep learning" + "fake," are synthetic media created using advanced machine learning techniques, particularly Generative Adversarial Networks (GANs) and more recently, diffusion models. Unlike traditional photo or video editing tools, which required significant human intervention and often left detectable artifacts, deepfakes automate the production of hyper-realistic images, voices, and videos that are virtually indistinguishable from authentic recordings (Chesney & Citron, 2019; Mirsky & Lee, 2021).

Originally developed for research and entertainment purposes, deepfakes have quickly proliferated into areas of high risk. Open-source platforms and low-cost software have democratized access to generative AI tools, allowing even non-experts to produce convincing synthetic media. As accessibility has grown, so too has the misuse of this technology, ranging from identity theft and executive impersonation in financial fraud to political disinformation campaigns and cyber-harassment (Vaccari & Chadwick, 2020).

1.2 Real-World Manifestations of Deepfake Fraud

The malicious use of deepfakes is no longer hypothetical. Several high-profile cases illustrate the gravity of the problem. In 2019, a UK-based energy firm lost nearly €220,000 when fraudsters used a deepfake audio to impersonate the voice of the CEO of its German parent company, in-