International Journal of Society Reviews (INJOSER)
Vol. 4 No. 2 (2026), pages: 239~251
https://injoqast.net/index.php/INJOSER
e-ISSN: 3030-802X

BEYOND CRIMINALISATION: DIGITAL VICTIMISATION AND VICTIM PROTECTION AGAINST AI DEEPFAKES IN INDONESIA

Kus Rizkianto[1], Siswanto[2], Estiana Nabila[3]
Faculty of Law, Universitas Pancasakti Tegal, Indonesia
Corresponding author:1 kus_rizkianto@upstegal.ac.id ; 2 siswanto@upstegal.ac.id ; estiananabil@upstegal.ac.id

ABSTRACT

Artificial intelligence (AI) deepfakes enable the convincing imitation of an individual's image or voice, creating risks that extend beyond the identification and punishment of offenders. This article examines how Indonesian law responds to digital victimisation and whether its remedies address reputational, psychological and social harm. Using normative legal research and a focused interdisciplinary literature review, it analyses the Electronic Information and Transactions Law, Personal Data Protection Law, Sexual Violence Crimes Law, the Criminal Code and criminal procedure reforms, including the 2026 Witness and Victim Protection Law. The analysis identifies three interconnected problems: harm may arise before distribution; protection depends on fitting conduct within fragmented offences; and criminal proceedings alone do not ensure rapid content containment or sustained recovery. It proposes a victim-centred response linking accessible reporting, lawful evidence preservation, timely platform action, risk-sensitive support and restitution where legal conditions are met. Rather than claiming an absence of relevant laws, the article argues that coordination and remedies should reflect the continuous nature of technology-facilitated harm. This framework offers a policy-oriented contribution to debates on digital victimology and access to justice in Indonesia.

Keywords: deepfake; digital victimology; victim protection; artificial intelligence; Indonesia.

INTRODUCTION

Synthetic audiovisual media generated or manipulated through artificial intelligence have transformed the social meaning of visible and audible identity. A person's apparent voice, face or conduct can be reproduced without the underlying event having occurred. The resulting content can be satirical, educational or creative; its legal significance therefore cannot be inferred from the use of AI alone. The problem addressed here is harmful and unauthorised manipulation, especially when a recognisable individual is impersonated, demeaned or exposed to threats. The social consequences may emerge immediately upon discovery of an image, even before it is widely circulated. Digital identity is not merely information about an individual: it is also connected to personal autonomy, reputation, social relationships and the ability to participate safely in public life (Chesney and Citron 2019; Maddocks 2020).