

CHAPTER I

INTRODUCTION

1.1.BACKGROUND OF STUDY

Crimes involving technology are no longer unfamiliar to active users of digital products in this era. Large-scale hacking incidents, for example, have caused significant harm to individuals and State," institutions. Similarly, the prevalence of online gambling has been on the rise. In the era of globalization and the Industrial Revolution, particularly with technological advancements, opportunities for unlawful activities have significantly increased. One notable example is the misuse of deepfake technology, which has become widespread and is now considered one of the most serious crimes involving Artificial Intelligence (AI).

Deepfake is a form of artificial intelligence (AI) designed to create highly realistic photos, audio, and videos capable of deceiving viewers. It utilizes advanced machine learning and AI techniques to manipulate and generate content, often with the potential to mislead or misinform audiences.¹

As of 2023, there have been 95,820 media created illegally with AI-based applications that have then spread globally.² In addition, 825 incidents have been recorded with this AI as recorded in the AIID (AI Incident Database).³ This point raises concerns due to the potential for misuse, leading to the dissemination of deceptive content, privacy violations, and numerous

¹Ian P. McCarthy et al., "DeepFake: Trick or Treat?," *Elsevier*,(2019): 1, https://core.ac.uk/outputs/250590695/?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1.,

²Krjogja.com, "Masyarakat Diminta Waspadai Penyalahgunaan Deepfake, Apa Itu?," Krjogja/Nasional, 2023, <https://www.krjogja.com/nasional/1243298466/masyarakat-diminta-waspadai-penyalahgunaanDeepFake-apa-itu.> , Accessed at 14 August 2024

³AI Incident Database, "Incident List," AIID, 2024, [https://incidentdatabase.ai/summaries/incidents/.](https://incidentdatabase.ai/summaries/incidents/), Accessed at 22 October 2024

opportunities for criminal acts that are certain to cause significant harm to the public.

As found in several cases, among others, which occurred in March 2024, this case occurred in the Spanish city of Almandralejo, where there were indecent photos of a 14-year-old girl that were rumored to have been circulating for several weeks in groups made by other school children. This incident caused great anxiety for the victim's family, as expressed by Miriam Al-Adib, who is the mother of the victim. "Our concern is that these images have reached pornographic sites that we still do not know about."⁴

The worries surrounding Deepfake did not stop there. Another incident occurred in May 2024, involving fraud targeting a multinational design and engineering company in the UK, resulting in significant losses for the company. As explained by the company's spokesperson, the firm became a victim of fraud using Deepfake techniques, which led one of its staff members in Hong Kong to pay the perpetrators a sum of US \$25 million, equivalent to approximately 400 billion Rupiah. Although the company did not provide further details about the case, they confirmed that fake voices and images were used.⁵

From this, it can be understood that the rapid advancements in artificial intelligence (AI) technology have brought serious consequences. Applications designed to create fake content are now widely available. This has led to an increased risk of spreading false content, including the creation of pornographic videos and fake videos involving individuals who have no connection to the content. It has also significantly raised the potential for increased crime rates.

⁴ Kompas.com, "Skandal Aplikasi Pornografi 'Deepfake' Guncang Kota Kecil Spanyol dan AS," KOMPAS.com/Global, 2024, <https://www.kompas.com/global/read/2024/03/01/160000370/skandal-aplikasi-pornografi-deepfake-guncang-kota-kecil-spanyol-dan-as?page=all>., Accessed at 18 August 2024

⁵ CNN Indonesia, "Perusahaan Inggris Kena Tipu, Transfer Rp400 M Gara-gara Deepfake," CNN Indonesia/Teknologi/Teknologi Informasi, 2024, <https://www.cnnindonesia.com/teknologi/20240517131238-185-1098903/perusahaan-inggris-kena-tipu-transfer-rp400-m-gara-gara-deepfake>., Accessed at 18 August 2024

Such crimes should be considered serious when analyzed through the lens of Islamic law, particularly *Fiqh Jinayah*. *Fiqh Jinayah*, a branch of Islamic law, addresses criminal acts or offenses based on *Shar'i* evidence. Its principles encompass various crimes, including murder, theft, robbery, adultery (*zina*), false accusations of adultery (*qazf*), and others.

The creation of illegal media that harms the accused by portraying them in indecent acts, such as defamation, is regarded as a criminal offense under the principles of *Fiqh Jinayah*. In Islam, defamation is considered more severe than murder, as Allah SWT states in Surah Al-Baqarah, verse 191:⁶

وَالْفِتْنَةُ أَشَدُّ مِنَ الْقَتْلِ

Translations:

“For persecution is far worse than killing”

As in other cases, this incident has also caused significant losses for the victims. Based on its criminal elements, it should be treated as a serious matter under Islamic law.

Based on the analysis, this study aims to provide a clearer understanding of how Islam adjudicates contemporary cases arising from the impact of technological globalization, such as the Deepfake phenomenon.

Consequently, this study will focus on a legal review of Deepfake crimes, particularly those involving AI-generated pornography, under the title: ‘An Analysis of Crimes Using Deepfake Technology from The Perspective of *Fiqh Jinayah*.’ This study aims to enhance public digital literacy by offering a legal perspective on contemporary phenomena and the consequences of such actions, which is essential for addressing the challenges posed by globalization.

According to the Chairman of the Indonesia Cyber Security Forum (ICSF), digital forensics is one method that can be employed to provide legal

⁶ Q.S. Al – Baqarah: 191

evidence in Deepfake cases.⁷ Furthermore, the government must intensify efforts to raise awareness about the existence of Deepfake technology at all levels of society. Therefore, enhancing public literacy on issues related to Deepfake is of paramount importance.

1.2.FORMULATION OF THE PROBLEM

Based on the background of study above, the following research questions can be formulated:

- 1) What are the form of crimes based on the DeepFake technology?
- 2) How is *Fiqh Jinayah* perspective on crimes based on the DeepFake technology?

1.3.OBJECTIVE OF RESEARCH

Based on the formulation of the problem above, the objectives of this research can be outlined as follows:

1. To knowing the forms of crimes based on the DeepFake technology.
2. To knowing *Fiqh Jinayah* perspective on crimes based on the DeepFake technology

1.4.BENEFIT OF RESEARCH

1.4.1. Theoretical Significance

This research contributes to the development of Islamic legal understanding regarding contemporary phenomena, such as the emergence of DeepFake as a result of technological globalization. Specifically, it aims to enhance literacy related to the principles of *Fiqh Jinayah* in addressing contemporary phenomena influenced by technological globalization.

1.4.2. Practical Significance

⁷Cyberthreat.id, "Penyalahgunaan Deepfake Bisa Dijerat UU ITE, Tapi....," Cyberthreat.id/News, 2019, <https://cyberthreat.id/read/3323/Penyalahgunaan-DeepFake-Bisa-Dijerat-UU-ITE-Tapi.>, Accessed at 5 July 2024

The purpose of this study is to increase public awareness of the need for prudence when using social media, especially among frequent users. This is particularly important in the context of AI-driven technological globalization in order to protect others and to steer clear of potentially illegal activities, like the more common DeepFake incidents.

1.5.LITERATURE REVIEW

Name	Title	Research Method	Analysis Result	Research Similarity	Novelty
Faras Paria, 2024	Fenomena Deepfake Di Era Teknologi Informasi Perspektif Al-Qur'an (Studi Analisis Q.S Al-Baqarah Ayat 42)	Qualitative Research	Interpretation of Verse 24 of Surah Al-Baqarah Regarding the DeepFake Phenomenon	DeepFake Technology Crime, Research Method	The Researcher's Review is Not Limited to a Specific Verse of the Qur'an but Focuses on <i>Fiqh Jinayah</i> ⁸
Nabila Syahrani Lestari, 2024	Kebijakan Formulasi Hukum Pidana Atas Praktik Deepfake Dilihat Dari Perspektif Kejahatan Siber Dan Pornografi	Qualitative Research	Regulatory Gaps Regarding Crimes Involving DeepFake Practices in Indonesia	Legal Perspective of Crime Based on the DeepFake Technology, Research Method	Examination of Crimes Involving DeepFake Practices Focused on the

⁸ Faras Paria, "Fenomena Deepfake Di Era Teknologi Informasi Perspektif Al-Qur'an (Studi Analisis Q.S Al-Baqarah Ayat 42)" (Universitas Islam Negeri Raden Fatah Palembang, 2024). <https://repository.radenfatah.ac.id/40838/>.

					Principles of <i>Fiqh Jinayah</i> ⁹
Muhammad Isnaeni Puspito, 2023	Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Kejahatan Pornografi Online (Cyberporn) di Indonesia	Qualitative Research	Analysis of Positive Law Related to CyberPorn Crimes in Indonesia	Legal Perspective of Cyberporn Crimes, Research Method	Review of Islamic Law (Principles of <i>Fiqh Jinayah</i>) on the Creation of Media Using AI-Based Applications: A Case Study on DeepFake ¹⁰
Kinanti Cahya Lintang, 2021	Tinjauan Hukum Pidana Islam Terhadap Cyber Crime dalam Bentuk Pencurian Data Pribadi	Qualitative Research	The Application of Sanctions Against Cybercrime Perpetrators in the Form of	Islamic Legal Perspective of Cyber Crime, Reserach Method	A Study Specifically on the Application of DeepFake: An Analysis Based on <i>Fiqh Jinayah</i> ¹¹

⁹ Nabila Syahrani Lestari, “*Kebijakan Formulasi Hukum Pidana Atas Praktik Deepfake Dilihat Dari Perspektif Kejahatan Siber Dan Pornografi*” (Palembang, Universitas Sriwijaya, 2024).

¹⁰ Muhammad Isnaeni Puspito, *Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Kejahatan Pornografi Online (Cyberporn) Di Indonesia* (Semarang: STIEPARI Press, 2023), <https://badanpenerbit.stiepari.org/index.php/stieparipress/article/view/147>

¹¹ Khinanti Cahya Lintang, “Tinjauan Hukum Pidana Islam Terhadap Cyber Crime dalam Bentuk Pencurian Data Pribadi” (Surabaya, Universitas Islam Negeri Sunan Ampel, 2021).

			Personal Data Theft		
Sayid Muhammad Rifki Noval, 2019	Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi: Penggunaan Teknik DeepFake	Qualitative Research	Implementation of Rights as Regulated in Law No. 9 of 2016 on Amendments to Law No. 11 of 2008	Legal Perspective of Crimes Based On The DeepFake Technology, Research Method	Implementation of <i>Fiqh Jinayah</i> Principles in the Misuse of Personal Data to Illegally Create Media Using DeepFake Methods ¹²

Broadly, this study distinguishes itself from previous studies by focusing on the analysis and application of *Fiqh Jinayah* principles to crimes emerging from globalization and technological advancements, with particular emphasis on the phenomenon of Deepfake.

1.6. RESEARCH METHOD

1.6.1. Type of Research

This study employs a qualitative study method combined with a normative juridical approach. The approach involves study procedures to produce descriptive data relevant to Deepfake and *Fiqh Jinayah*.¹³

¹² Sayid Muhammad Rifki Noval, "Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi: Penggunaan Teknik Deepfake," (Universitas Islam Nusantara Bandung, 2019).

¹³ Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020), 28

Normative juridical research is a legal research that does not touch or enter the area of empirical or sociological law for data collection data it needs.¹⁴

The selection of this research type is driven by the need to analyze existing legal norms while addressing contemporary issues that lack clarity. It aims to establish a robust theoretical framework for legal studies by comprehensively understanding prevailing norms and legal principles.

1.6.2. Data Sources

This study utilizes secondary data derived from written sources, encompassing primary, secondary, and tertiary legal materials related to the issue of DeepFake. The choice of secondary data is guided by several factors, including time efficiency, ease of accessibility, and its relevance to the theoretical framework. This approach enables the researcher to conduct the study effectively and comprehensively.¹⁵

The legal materials to be used are:

1.6.2.1. Primary legal materials

Books:

(١) الحدود والتعزيرات عند ابن القيم (بكر بن عبد الله أبو زيد)

(٢) المطلاع على دقائق زاد المستقنع فقه الجناية والحدود (عبد الكريم بن م

حمد اللاحم)

(٣) كتاب التشريع الجنائي مقارنة بالقانون الوضعي (عبد القادر عودة)

(٤) الفقه الإسلامي و أدلته (وحبة الزحيلي)

(٥) موسوعة الإجماع في الفقه الإسلامي (مجموعة من المؤلفين)

¹⁴ Nurul Qamar, *Metode Penelitian Hukum*, (Makassar: CV. Social Politic Genius, 2020),

¹⁵ Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020), 59

1.6.2.2. Secondary legal materials

The secondary legal materials utilized in this research include scientific references such as legal journals, books, academic manuscripts, and hearing records, all of which pertain to the research focus on technology-based crimes, Deepfake, and *Fiqh Jinayah*.

1.6.3. Data Collection Method

The data collection methods used in this study are literature review, document analysis, and archive studies. These involve gathering data from written materials as documents, such as books containing opinions, theories, arguments, or legal rulings, including primary legal materials, secondary legal materials, tertiary legal materials, and non-legal materials related to technology-based crimes, particularly DeepFake and *Fiqh Jinayah*.¹⁶

The rationale for choosing this data collection method is that it allows for an in-depth examination of legal materials through various means such as reading, observation, and online research.

1.6.4. Data Analysis Method

In analyzing the data, the researcher employs a qualitative descriptive analysis method namely by interpreting the legal materials that have been processed. The use of this interpretation method aims to interpret the law, whether the legal material, especially primary legal material, contains a vacuum of legal norms, antinomy of legal norms and vague legal norms.¹⁷ Then in this research by thoroughly examining the definitions and practices of DeepFake as well as the principles of *Jinayah* in *Fiqh Jinayah*. Subsequently, the principles of *Fiqh Jinayah* are applied to the practice of DeepFake, highlighting the correlation between the two.

1.7. SYSTEMATIC WRITING

The writing methodology outlines the content of the research, which is divided into four chapters. Chapter I introduces the study, including the

¹⁶ Ibid. 64

¹⁷ Wiwik Sri Widiarty. *Metode Penelitian Hukum*. (Yogyakarta: Publika Global Media, 2024), 132

Background of the Research, Problem Statement, Research Objectives, Research Benefits, and the Systematic Structure of Writing. Chapter II reviews previous studies and theoretical frameworks related to DeepFake, and theoretical perspectives on *Fiqh Jinayah*. Chapter III analyzes DeepFake practices and applies the principles of *Fiqh Jinayah* to crimes based on the DeepFake Technology. Finally, Chapter IV presents the conclusions of the research, including findings on DeepFake practices based on *Fiqh Jinayah*, along with recommendations and closing remarks.

