

**ANALISIS PENYALALAHGUNAAN *DEEPPAKE* DALAM
PERSPEKTIF HUKUM PIDANA ISLAM
SKRIPSI**



Diajukan Oleh:

AZZUMARDIAZRA
NIM. 220104076

**Mahasiswa Fakultas Syariah dan Hukum
Prodi Hukum Pidana Islam**

**FAKULTAS SYARIAH DAN HUKUM
UNIVERSITAS ISLAM NEGERI AR-RANIRY
2026**

**ANALISIS PENYALALAHGUNAAN *DEEPFAKE* DALAM PERSPEKTIF
HUKUM PIDANA ISLAM**

SKRIPSI

Diajukan Kepada Fakultas Syari'ah dan Hukum
Universitas Islam Negeri Ar-Raniry Dasrussalam Banda Aceh
Sebagai Salah Satu Beban Studi Program Sarjana (S-1)
Dalam Ilmu Hukum Pidana Islam

Oleh:

AZZUMARDI AZRA

NIM. 220104076

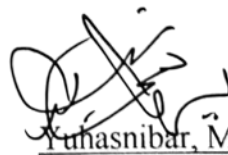
Disetujui untuk Dimunaqasyahkan oleh:

Pembimbing I,



Prof. Dr. Ali Abubakar, M.Ag
NIP. 197101011996031003

Pembimbing II,



Yunasnibar, M.Ag
NIP. 197908052010032002

ANALISIS PENYALALAHGUNAAN *DEEFAKE* DALAM PERSPEKTIF HUKUM PIDANA ISLAM

SKRIPSI

Telah Diuji oleh Panitia Penguji Tugas Akhir Skripsi
Fakultas Syariah dan Hukum UIN Ar-Raniry
dan Dinyatakan Lulus Serta Diterima
Sebagai Salah Satu Beban Studi Program Sarjana (S-1)
Pada Program Studi Hukum Pidana Islam

Pada Hari/Tanggal: Senin, 14 Agustus 2026
1 Rabiul Awal 1448

PENGESAHAN SKRIPSI
Di Darussalam, Banda Aceh
Panitia Penguji Tugas Akhir Skripsi:

Ketua


Prof. Ali Abubakar, M.Ag
NIP. 197101011996031003

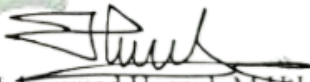
Sekretaris


Yubasnibar, M.Ag
NIP. 197908052010032002

Penguji I


Misran, S.Ag., M.Ag
NIP. 197507072006041004

Penguji II


Muhammad Husnul, M.P.I
NIP. 199006122020121013

Mengetahui


Dekan Fakultas Syariah dan Hukum
UIN Ar-Raniry Banda Aceh

Kamaruzzaman, M.Sy
NIP. 197809172009121006

PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan di bawah ini:

Nama : Azzumardi Azra

Nim 22010476

Prodi : Hukum Pidana Islam

Fakultas : Fakultas Syari'ah dan Hukum UIN Ar-Raniry

Dengan ini menjelaskan bahwa dalam penulisan skripsi ini, saya:

1. ***Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggung jawabkan;***
2. ***Tidak melakukan plagiasi terhadap naskah karya orang lain;***
3. ***Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya;***
4. ***Tidak melakukan manipulasi dan pemalsuan data;***
5. ***Mengerjakan sendiri dan mampu bertanggung jawab atas karya ini.***

Bila di kemudian hari ada tuntutan dari pihak lain atas karya saya melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap untuk dicabut gelar akademik atau diberikan sanksi lain berdasarkan aturan yang berlaku di Fakultas Syari'ah dan Hukum UIN Ar-Raniry.

Demikian surat pernyataan ini saya buat dengan sesungguhnya,

Banda Aceh, 10 Agustus 2026

Yang menyatakan



Azzumardi Azra

ABSTRAK

Nama : Azzumardi Azra
NIM : 220104076
Fakultas / Prodi : Syari'ah dan Hukum / Hukium Pidana Islam
Judul : Analisis Penyalahgunaan *Deepfake* dalam Perspektif Hukum Pidana Islam
Tanggal Sidang : 14 Agustus 2026
Tebal Skripsi : 84 Halaman
Pembimbing I : Prof. Dr. Ali Abubakar, M.Ag
Pembimbing II : Yuhasnibar, M.Ag
Kata Kunci : *Deepfake*, Kejahatan Siber, *Artificial Intelligence*

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) telah melahirkan teknologi *deepfake* yang mampu memanipulasi gambar, video, dan suara sehingga tampak autentik. Di satu sisi, teknologi ini memberikan manfaat dalam berbagai bidang, di sisi lain berpotensi disalahgunakan untuk melakukan tindak pidana seperti penipuan, pencemaran nama baik, pornografi, pelanggaran privasi, dan penyebaran informasi palsu. Permasalahan muncul karena hukum positif Indonesia belum memiliki pengaturan yang secara khusus mengatur tindak pidana *deepfake*, sehingga diperlukan kajian antara lain dari perspektif hukum pidana Islam. Penelitian ini bertujuan untuk menganalisis kasus-kasus penyalahgunaan *deepfake* sebagai tindak pidana di Aceh serta mengkaji kedudukan hukum *deepfake* menurut hukum pidana Islam. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Data diperoleh melalui studi kepustakaan terhadap bahan hukum primer, sekunder, dan tersier, kemudian dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa penyalahgunaan *deepfake* telah menimbulkan bentuk kejahatan siber, seperti penipuan, pencemaran nama baik, intimidasi digital, dan pelanggaran privasi. Meskipun belum terdapat pengaturan khusus mengenai *deepfake*, perbuatan tersebut dapat dijerat melalui ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik, Khususnya pada pasal 27 ayat (1), Undang-Undang Pornografi (UU No.44 Tahun 2008), Undang-Undang Perlindungan Data Pribadi No 27 Tahun 2022), dan Kitab Undang-Undang Hukum Pidana (UU No 1 Tahun 2023) Dalam perspektif hukum pidana Islam, penyalahgunaan *deepfake* memenuhi unsur jarimah ta'zir karena mengandung unsur kebohongan (al-kadzib), penipuan (at-tadlis), fitnah (buhtan), serta menimbulkan kemudharatan terhadap kehormatan, harta, dan hak-hak individu yang dilindungi oleh maqashid al-syari'ah. Oleh karena itu, diperlukan pembentukan regulasi yang lebih spesifik untuk memberikan kepastian hukum serta perlindungan yang efektif terhadap korban penyalahgunaan teknologi *deepfake*.

KATA PENGANTAR

بسم الله الرحمن الرحيم
الحمد لله، والصلاة والسلام على رسول الله وعلى آله وأصحابه ومن والاه، أما بعد

Segala puji dan syukur senantiasa Penulis ucapkan Kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya kepada penulis, sehingga Penulis dapat menyelesaikan skripsi yang berjudul “**Analisis Penyalahgunaan Deepfake Dalam Perspektif Hukum Pidana Islam**” Shalawat serta salam semoga tetap terlimpahkan kepada Nabi Muhammad Saw serta keluarga, para sahabat dan para pengikut beliau.

Skripsi ini dibuat sebagai salah satu syarat untuk menyelesaikan pendidikan pada Program Studi Hukum Pidana Islam Fakultas Syari’ah dan Hukum Universitas Islam Negeri Ar-Raniry Banda Aceh, serta untuk memenuhi kewajiban akademik guna memperoleh gelar (S1).

Dalam proses penyusunan skripsi ini, Penulis mendapatkan banyak ilmu, pengalaman, dan wawasan baru yang berharga. Tidak dapat dipungkiri, penyelesaian skripsi ini juga tidak terlepas dari bantuan dan dukungan berbagai pihak yang telah memberikan motivasi, nasihat, dan masukan selama proses penelitian dan Penulis. Oleh karena itu, dengan segala kerendahan hati, Penulis ingin menyampaikan rasa terima kasih yang tulus kepada:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya selama masa perkuliahan dan pengerjaan laporan tugas akhir ini. Karunia berupa kemudahan dan kelancaran dalam pengerjaan seperti kesehatan, kekuatan, waktu, serta iman dan islam yang menjadi salah satu faktor penting dalam terselesaikannya laporan tugas akhir ini dengan tepat waktu.
2. Kepada orang tua tercinta, Ayahanda Abdurrahman, dan Ibunda Nuraini yang selalu menjadi sumber kekuatan dan motivasi terbesar. Terima kasih

atas doa yang tak pernah putus, dukungan moral dan material yang tiada henti, serta cinta yang senantiasa menguatkan penulis untuk melangkah hingga menyelesaikan skripsi ini.

3. Kepada Pembimbing I Prof. Dr. Ali Abubakar, M.Ag, selaku dosen pembimbing yang telah meluangkan waktu untuk memberikan bimbingan, arahan, dan masukan yang sangat berarti dalam penyelesaian skripsi ini. Kepada Pembimbing II Ibu Yuhasnibar, S.Hi., M.Ag. yang dengan penuh kesabaran telah memberikan bimbingan, arahan, dan masukan dalam penyusunan skripsi ini.
4. Bapak Prof. Dr. Kamaruzzaman, M.Sh. selaku Dekan Fakultas Syariah dan Hukum.
5. Bapak Dedy Sumardi, M.Ag. selaku ketua prodi Hukum Pidana Islam dan Bapak Riadhus Sholihin, M.H selaku sekretaris prodi, beserta seluruh staf prodi.

Demikian skripsi ini saya tulis, dengan harapan agar dapat memberikan manfaat kepada masyarakat banyak khususnya kepada para pembacanya, serta menjadi bahan referensi bagi penelitian selanjutnya. Saya menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, saya sangat terbuka terhadap kritik dan saran yang membangun demi perbaikan di masa mendatang.

Banda Aceh, 10 Agustus
2026



Azzumardi Azra
220104076

TRANSLITERASI ARAB LATIN

Keputusan Bersama Menteri Agama Dan Menteri Pendidikan Dan Kebudayaan Republic Indonesia

No: 128 Tahun 1987-Nomor: 0543b/U/1987

Transliterasi dimaksudkan sebagai pengalih-hurufan dari abjad yang satu ke abjad yang lain. Transliterasi Arab-Latin ialah penyalinan huruf-huruf Arab dengan huruf-huruf Latin beserta perangkatnya.

A. Konsonan

Fonem konsonan Bahasa Arab yang dalam sistem tulisan Arab dilambangkan dengan huruf. Dalam transliterasi ini sebagian dilambangkan dengan huruf dan sebagian di lambangkan dengan tanda, dan sebagian lagi dengan huruf dan tanda sekaligus.

Berikut ini daftar huruf Arab yang dimaksudkan dan transliterasi dengan huruf latin:

Tabel 0.1: Tabel Transliterasi Konsonan

Huruf arab	Nama	Huruf latin	Nama
ا	Alif	Tidak dilambangkan	Tidak dilambangkan
ب	Ba	B	Be
ت	Ta	T	Te
س	Ša	š	es (dengan titik di atas)
ج	Jim	J	Je
ح	Ḥa	ḥ	ha (dengan titik di bawah)

خ	Kha	Kh	ka dan ha
د	Dal	D	De
ذ	Ḍal	ḏ	zet (dengan titik di atas)
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	es dan ye
ص	Ṣad	ṣ	es (dengan titik di bawah)
ض	Ḍad	ḍ	de (dengan titik di bawah)
ط	Ṭa	ṭ	te (dengan titik di bawah)
ظ	Za	ẓ	zet (dengan titik di bawah)
ع	'ain	'	koma terbalik (di atas)
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qaf	Q	Ki
ك	Kaf	K	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We

ها	Ha	H	Ha
ء	Hamzah	‘	Apostrof
ي	Ya	Y	Ye

1. Vokal

Konsonan Vokal Bahasa Arab, seperti vokal bahasa Indonesia, terdiri dari vokal tunggal atau monoftong dan vokal rangkap atau diftong. Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harakat, transliterasinya sebagai berikut:

Huruf Arab	Nama	Huruf Latin	Nama
َ	Fathah	A	A
ِ	Kasrah	I	I
ُ	Dammah	U	U

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harkat dan huruf, transliterasinya gabungan huruf, yaitu:

Tanda	Nama	Huruf Latin	Nama
اِيْ	Fathah dan ya	Ai	A dan I
اُوْ	Kasrah dan wau	Iu	I dan U

Contoh:

كَيْفَ = *kaifa*,

حَوْلَ = *hau-la*

2. Maddah

Maddah atau vokal panjang yang lambangnya berupa harkat dan huruf, transliterasinya berupa huruf dan tanda, yaitu:

Harkat dan Huruf	Nama	Huruf dan Tanda	Nama
اَ	Fathah dan alif atau ya	ā	a dan garis di atas
اِ	Kasrah dan ya	ī	i dan garis di atas
اُ	Ḍammah dan wau	ū	u dan garis di atas

Contoh:

مَا : *māta*

رَامِي : *ramā*

قِيلَ : *qīla*

يَامِيتُ : *yamītu*

3. Ta Marbūṭah

Transliterasi untuk *ta marbūṭah* ada dua bentuk, yaitu: *ta marbūṭah* yang hidup atau mendapat harkat *fathah*, *kasrah*, dan *ḍammah*, transliterasinya adalah [t]. Sedangkan *ta marbūṭah* yang mati ataupun mendapat penambahan harkat sukun, transliterasinya adalah [h]. Jika pada kata yang berakhir dengan huruf *ta marbūṭah*, diikuti oleh kata yang menggunakan kata sandang (*al-*), serta bacaan kedua kata itu terpisah, maka *ta marbūṭah* itu ditransliterasikan dengan *ha* (h).

Contoh:

رَوْدَةُ الرَّحْمَنِ : *raudah al-atfāl*

لَمَدِينَةِ الْفَضْلِ : *al-madīnah al-fāḍilah*

لِحِكْمَةٍ : *al-ḥikmah*

4. Syaddah (Tasydīd)

Syaddah atau disebut dengan kata *tasydīd* yang dalam sistem tulisan Arab dilambangkan dengan satu tanda *tasydīd* (ˤ) dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda *syaddah*, misalnya di dalam contoh berikut:

رَبَّنَا : *rabbānā*

نَجَّيْنَا : *najjainā*

لَحَقْ : *al-ḥaqq*
 لَحَجْ : *al-ḥajj*
 ن : *nu‘ima*
 اُدْوَوْن : *‘aduwwun*

Jika huruf ي memiliki *tasydīd* di akhir suatu kata, dan kemudian didahului oleh huruf berharakat kasrah (◌ِ), maka ia ditransliterasi seperti huruf *mādah* (ī).

Contoh:

عَلِي : ‘*Alī* (bukan ‘*Aliyy* atau ‘*Aly*)
 عَرَبِي : ‘*Arabī* (bukan ‘*Arabiyy* atau ‘*Araby*)

5. Kata Sandang

Kata sandang dalam sistem tulisan Arab dilambangkan dengan huruf ال (*alif lam ma‘rifah*). Pada pedoman transliterasi ini, kata sandang ditransliterasi seperti biasa yaitu (*al-*), baik ketika ia diikuti oleh huruf *syamsiah* maupun huruf *qamariah*. Kata sandang tersebut tidaklah mengikuti bunyi huruf langsung yang mengikutinya. Kata sandang itu ditulis terpisah dari kata yang mengikutinya dan dihubungkan dengan garis mendatar (-). Contohnya:

الشَّمْسُ : *al-syamsu* (bukan *asy-syamsu*) ة
 الزَّلْزَلَةُ : *al-zalzalah* (bukan *az-zalzalah*) ة
 الفَلْسَفَةُ : *al-falsafah*
 الْبِلَادُ : *al-bilādu*

6. Hamzah

Aturan transliterasi huruf hamzah menjadi apostrof (‘) hanya berlaku bagi hamzah yang terletak di tengah dan akhir kata. Namun, bila hamzah terletak di awal kata, ia tidak dilambangkan, karena di dalam tulisan Arab ia berupa alif. Contohnya:

تَأْمُرُونَ : *ta‘murūna*

النَّوْءُ : *al-nau'*

سَيَائُون : *syai'un*

أُمِرْتُ : *umirtu*

7. Penulisan Kata Arab yang Lazim digunakan dalam Bahasa Indonesia

Kata, istilah, atau kalimat Arab yang ditransliterasikan adalah kata, istilah atau kalimat yang belum dibakukan dalam bahasa Indonesia. Kata, istilah atau kalimat yang telah lazim dan menjadi bagian dari perbendaharaan dalam bahasa Indonesia, atau sudah sering ditulis di dalam tulisan bahasa Indonesia, tidak lagi ditulis menurut cara transliterasi di atas. Misalnya kata Alquran dari *al-Qur'ān*, sunah, hadis, khusus dan juga umum. Namun bila kata-kata tersebut menjadi bagian dari satu rangkaian teks Arab, maka mereka harus ditransliterasikan secara utuh. Contoh:

فِي زِيلَالِ الْقُرْآنِ

: *Fī Zilāl al-Qur'ān*

الْسُّنَّةُ قَبْلَ التَّأْدِينِ

: *Al-Sunnah Qabla al-Tadwīn*

Al- 'ibārāt fī 'umūm al-lafz lā bi-khuṣūṣ al-sabab

9. Lafz al-Jalālah (الله)

Kata “Allah” yang didahului partikel seperti huruf *jarr* dan huruf lainnya atau berkedudukan sebagai *muḍāf ilaih* (frasa nominal), ditransliterasikan tanpa huruf hamzah. Contoh:

بَيْنَ اللَّهِ

: *dīnullāh*

Adapun *ta marbūṭah* di akhir kata yang disandarkan pada *lafz al-jalālah*, ditransliterasikan dengan huruf (*t*). Contoh:

هُمْ فِي رَحْمَةِ اللَّهِ : *hum fī rahmatillāh*

10. Huruf Kapital

Walau sistem tulisan Arab tidak mengenal huruf kapital (*All Caps*), dalam transliterasinya huruf-huruf tersebut dikenai ketentuan tentang penggunaan huruf capital berdasarkan pedoman ejaan Bahasa Indonesia yang

berlaku atau Ejaan Yang Disempurnakan (EYD). Huruf capital, misalnya, digunakan untuk menuliskan huruf awal nama diri (orang, tempat, bulan) dan

huruf pertama pada permulaan kalimat. Bila nama diri didahului oleh kata sandang (*al-*), maka yang ditulis dengan huruf capital tetap huruf awal nama diri tersebut, bukan huruf awal kata sandangnya. Jika terletak pada awal kalimat, maka huruf A dari kata sandang tersebut menggunakan huruf capital (*Al-*). Ketentuan yang sama juga berlaku untuk huruf awal dari judul referensi yang didahului oleh kata sandang (*al-*), baik ketika ia ditulis dalam teks maupun dalam catatan rujukan (CK, DP, CDK, dan DR). Contoh:

Wa mā Muḥammadun illā rasūl

Inna awwala baitin wuḍi’a linnāsi lallaẓī bi Bakkata mubārakan

Syahru Ramadān al-laẓī unzila fīh al-Qur’ān

Nasir al-Dīn al-Ṭūs

Abu Naṣr al-Fārābī

Al-Gazālī

Al-Munqiz min al-Ḍalāl.



DAFTAR LAMPIRAN

Lampiran 1	: SK Penetapan Pembimbing Skripsi	78
------------	---	----



DAFTAR ISI

PENGESAHAN SIDANG	ii
PERNYATAAN KEASLIAN KARYA ILMIAH.....	iii
ABSTRAK	iv
KATA PENGANTAR	v
BAB SATU.....	1
PENDAHULUAN.....	1
A. Latar belakang masalah.....	1
B. Rumusan Masalah.....	6
C. Tujuan Penelitian	6
D. Penjelasan Istilah	6
E. Kajian Pustaka	8
F. Metodologi Penelitian	11
G. Sistematika Pembahasan	15
BAB DUA.....	16
PENYALAHGUNAAN DEEPPAKE SEBAGAI TINDAK PIDANA	16
A. Konsep Deepfake	16
B. Tindak Pidana (<i>Jarimah</i>).....	27
C. Teori Kejahatan Siber (<i>Syber Crime</i>).....	31
BAB TIGA TINJAUAN HUKUM PIDANA ISLAM TERHADAP PENYALAHGUNAAN TEKNOLOGI DEEPPAKE.....	37
BAB EMPAT	63
PENUTUP.....	63
DAFTAR PUSTAKA.....	66

BAB SATU

PENDAHULUAN

A. Latar belakang masalah

Perkembangan teknologi digital di masa modern sudah melahirkan bermacam inovasi, salah satunya merupakan kemunculan teknologi *deepfake*, *deepfake* ialah hasil penggabungan antara kecerdasan buatan(AI) serta metode *deep learning*, yang sanggup menciptakan manipulasi visual serta audio yang sangat realistis. Teknologi ini membolehkan seorang nampak mengucapkan ataupun melaksanakan suatu dalam video yang sesungguhnya tidak sempat terjalin.¹

Perkembangan serta pertumbuhan teknologi kecerdasan buatan (*Artificial intelligence/AI*) dengan seiringnya waktu terus berkembang sangat pesat khususnya dalam beberapa dekade terakhir dan membawa dampak yang sangat signifikan, Fenomena ini awalnya dimanfaatkan sebagai hiburan serta teknologi film, namun kini telah menjelma menjadi ancaman baru didalam dunia digital, khususnya disaat disalahgunakan untuk tindakan kriminal serta kejahatan siber.²

Sayangnya, kecepatan adopsi teknologi *deepfake* tidak sebanding dengan literasi digital masyarakat, sehingga membuka celah yang sangat besar dalam penyalahgunaan dan kerugian yang tidak sedikit, baik secara moral maupun materil. Salah satu wujud penyalahgunaan *deepfake* yang sangat mengkhawatirkan ialah dalam bidang pornografi. Konten *deepfake* pornografi kerap melibatkan penggunaan wajah, yang mana Teknologi *deepfake* dapat dengan sangat mudah memanipulasi, menukar, meniru ekspresi, pola atau mimik, dan suara orang lain,

¹ Putu. "Peran *Artificial Intelligence (AI)* Untuk Mendukung Pembelajaran Di Masa Pandemi Covid - 19."vol 1 No 1 (2022)

² Natanael Hiskia Mongkau, Herlyanty Y.A. Bawole, Altje A. Musa, *Penegakan Hukum Terhadap Penyalahgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Kedalam Gambar Atau Vidio Porno*, Jurnal Fakultas Hukum Unsrat Vol 13 No. 2 ,2025, hlm 2

sehingga seakan-akan ekspresi, gerak tubuh, atau suara yang dihasilkan itu terlihat seakan akan sangat nyata. karena hal tersebut, konten konten yang dihasilkan *deepfake* ini sangat mudah untuk menjadi trending topik sehingga dapat menimbulkan kerugian yang besar terhadap nama baik dan martabat korban, dan dapat merusak reputasi seseorang³, alasan dibuatnya konten-konten semacam ini sangat beragam mulai hanya untuk kepentingan pribadi, alasan komersial untuk dijual atau diunggah kepada akun akun yang menerima *endorsement*, atau hanya untuk tujuan balas dendam kepada si korban⁴,

Kemudian penyebaran konten konten *deepfake* melalui media sosial juga sangat mempercepat dampak negatifnya secara sosial hal ini menjadi perhatian utama dalam hukum positif di Indonesia karena terkait langsung dengan perlindungan terhadap kehormatan, privasi, dan moral publik.

Fenomena penyalahgunaan *deepfake* menimbulkan masalah yang serius, diantaranya meningkatnya kasus kasus pencemaran nama baik melalui media sosial, penyebaran video palsu di kalangan pelajar dan mahasiswa, serta kasus kasus hukum yang sulit diselesaikan karena keterbatasan regulasi spesifik. Hal ini mencerminkan adanya ketimpangan antara kemajuan teknologi dan kesiapan sistem hukum serta etika sosial untuk menghadapinya.

Pada saat ini di Indonesia, kasus penyalahgunaan *deepfake* semakin marak terjadi, salah satu kasus yang dapat kita ambil contoh ialah kasus penggunaan wajah presiden ke 8 Indonesia yaitu bapak Prabowo Subianto, pelaku menggunakan wajah dari bapak Prabowo dengan menggunakan aplikasi *deepfake* untuk menipu korban dengan menawarkan bantuan pemerintah, namun dengan dalih harus mentransfer uang terlebih dahulu, kemudian untuk lebih menyakinkan

³ Antika Setia Dewi, Dian Alan Setiawan, *Penegakan Hukum Terhadap Pelaku Deepfake Porn Dihubungkan Hukum Pidana Positif di Indonesia*, Bandung Conference Series: Law Studies, Vol 4, No 1 (2024) hlm 510

⁴ Isnaini Imroatus, "Protection of Victims of Deep Fake Pornografi in a Legal Perspective in Indonesia," *International Journal of Multicultural and Multireligious Understanding*, International Journal of Multicultural and Multireligious Understanding, 10, no. 1 (Januari 2023).

si korban, pelaku juga menggunakan wajah dari wakil presiden Indonesia ke 8, bapak Gibran Rakabuming Raka, dan menteri keuangan ibu sri mulyani, akibatnya lebih dari 100 orang dari 20 provinsi menjadi korban keganasan pelaku, dengan total kerugian mencapai 65 juta, kasus ini dapat diungkap Direktorat Tindak Pidana Siber Bareskrim Polri di lampung tengah pada januari⁵

Di Aceh juga terdapat beberapa kasus penyalahgunaan *deepfake*, yang menonjol adalah teror terhadap penggiat kemanusiaan dan influencer Afina Syifa pada awal tahun 2026, Dia mendapatkan intimidasi berupa foto tanpa busana hasil rekayasa *deepfake* dan serangan akun palsu yang mengatasnamakan ayahnya, setelah mengkritik kondisi sekolah pasca banjir di Aceh, yang disebut belum pulih yang mana masih beroperasi di tenda-tenda. Kasus ini menambah daftar panjang insiden intimidasi digital terhadap kreator konten di wilayah Sumatra.⁶

Kemudian kasus yang dialami Kasi Pammat Direktorat Samapta Polda Aceh, Kopol Sudianto, yang mana foto, video, serta suaranya diambil untuk menipu para kerabat oleh oknum yang tidak bertanggung jawab dengan modus yang dijalani pelaku sangat bervariasi mulai dengan memita pinjaman mendesak hingga menawarkan penjualan mobil mewah, dalam 3 hari banyak korban terkelabui dan mengirim sejumlah uang sebelum menyadari adanya rekayasa.⁷

Meskipun hingga saat ini belum terdapat satu regulasi yang secara spesifik menyebut istilah *deepfake* namun beberapa ketentuan perundang-undangan nasional dapat digunakan untuk menjerat pelakunya. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 27 ayat (1), menjerat perbuatan penyebaran konten asusila melalui media elektronik, dan Pasal 35 mengatur mengenai manipulasi data elektronik. Selain itu, UU Pornografi (UU

⁵ Media Bangsa, “Deepfake Prabowo Jadi Modus Penipuan Marak Awal 2025”, 3 Januari 2026, diakses 23 Juni 2026, <https://mediabangsa.co.id/deepfake-prabowo-jadi-modus-penipuan-marak-awal-2025/>.

⁶ Nukilan, “Foto Hasil Rekayasa AI Dikirim untuk Mengancam Relawan Kemanusiaan di Aceh”, 30 Mei 2026, diakses pada 23 Juni 2026, <https://nukilan.net/deepfake-digunakan-untuk-membungkam-kritik-di-aceh/>.

⁷ Serambi News, “Modus Penipuan Menggunakan Teknologi Deepfake Terjadi di Aceh Timur”, 16 Oktober 2025, diakses pada 23 Juni 2026, <https://serambinews.com/berita/modus-penipuan-menggunakan-teknologi-deepfake-terjadi-di-aceh-timur>.

No. 44 Tahun 2008), UU Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022), serta KUHP Baru (UU No. 1 Tahun 2023) turut memberikan sanksi pidana atas perbuatan yang mencemarkan nama baik, menyebarkan konten cabul, atau menyalahgunakan data pribadi.

Meskipun berbagai peraturan perundang-undangan tersebut dapat dijadikan landasan untuk menindak lanjuti pelaku penyalahgunaan *deepfake*, namun keberadaan regulasi tersebut pada dasarnya masih bersifat umum dan secara khusus belum mengatur karakteristik dan modus kejahatan *deepfake*, dalam UU ITE misalnya ketentuan terkait manipulasi informasi elektronik sebagaimana diatur di dalam Pasal 35, dapat digunakan untuk menjerat pelaku *deepfake*, namun Pasal 35 tersebut, belum secara tegas mengatur terkait manipulasi wajah, suara, maupun identitas digital seseorang yang dihasilkan melalui teknologi kecerdasan buatan (AI), demikian pula dengan UU Pornografi yang hanya bisa diterapkan ketika pelaku membuat konten yang mengandung unsur pornografi, sehingga tidak mencakup berbagai bentuk penyalahgunaan lainya seperti penipuan, pemerasan, pencemaran nama baik, dan penyebaran informasi palsu.

Sementara dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada dasarnya memberikan perlindungan terhadap penggunaan data pribadi tanpa persetujuan pemiliknya. Akan tetapi, regulasi tersebut belum secara spesifik mengatur penggunaan data pribadi yang diolah menjadi konten digital palsu yang menyerupai identitas seseorang melalui teknologi *deepfake*. Dalam praktiknya, pelaku sering mengambil data tersebut dari media sosial atau platform digital lainnya untuk kemudian diolah menggunakan kecerdasan buatan, begitu pula dengan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru) yang lebih berfokus pada akibat penyebaran berita bohong, bukan pada tindakan yang ditimbulkan, seperti penyebaran berita bohong, pencemaran nama baik, serta penipuan, bukan pada tindakan pembuatan dan manipulasi konten *deepfake* itu sendiri. Akibatnya, penegakan hukum terhadap pelaku *deepfake* masih

bergantung pada penafsiran berbagai ketentuan yang tersebar dalam beberapa peraturan perundang-undangan.

Kondisi tersebut menunjukkan bahwa perkembangan teknologi *deepfake* berjalan lebih pesat dibandingkan dengan perkembangan regulasi yang mengatur *deepfake* itu sendiri, padahal kemampuan teknologi *deepfake* ini berpotensi menimbulkan berbagai macam kerugian, baik terhadap perlindungan individu, masyarakat, maupun negara.

Oleh karena itu, diperlukan kajian mendalam mengenai penyalahgunaan *deepfake*, tidak hanya dalam perspektif hukum positif, tetapi juga dari perspektif hukum pidana Islam, guna memahami kedudukan hukumnya, menentukan bentuk jarimah yang sesuai, serta menganalisis konsep pertanggungjawaban dan sanksi yang dapat dikenakan terhadap pelakunya. Meskipun istilah *deepfake* tidak dikenal secara eksplisit dalam literatur fiqh klasik, substansi perbuatannya memiliki keterkaitan dengan unsur kebohongan (*al-kadzib*), penipuan (*at-tadlis*), fitnah, serta kemudaratan (*adh-dharar*) yang dilarang dalam syariat Islam. Selain itu, penyalahgunaan teknologi tersebut berpotensi menimbulkan kerugian terhadap kehormatan, harta, dan hak-hak individu yang termasuk dalam aspek-aspek yang dilindungi oleh tujuan syariat (*maqashid al-syariah*). Dengan demikian, fenomena *deepfake* tidak hanya menimbulkan permasalahan dalam ranah hukum positif, tetapi juga memunculkan persoalan hukum Islam yang memerlukan pengkajian secara komprehensif. Berdasarkan hal tersebut, penelitian yang berjudul **“Analisis Penyalahgunaan Deepfake dalam Perspektif Hukum Pidana Islam”** penting untuk dilakukan sebagai upaya memperoleh pemahaman yang lebih mendalam mengenai kedudukan hukum *deepfake*, klasifikasi jarimah yang relevan, serta konsep pertanggungjawaban dan sanksi yang dapat diterapkan terhadap pelakunya menurut hukum pidana Islam.

B. Rumusan Masalah

Dari latar belakang masalah maka penulis merumuskan permasalahan yang akan di teliti sebaga berikut:

- 1) Bagaimana Analisis kasus-kasus Penyalahgunaan *Deepfake*?
- 2) Bagaimana Penyalahgunaan *deepfake* menurut hukum pidana Islam?

C. Tujuan Penelitian

- 1) Untuk menganalisis bagaimana kasus-kasus Penyalahgunaan *deepfake*?
- 2) Untuk Mengkaji bagaimana penyalahgunaan *deepfake* menurut hukum pidana Islam?

D. Penjelasan Istilah

- 1) Tindak Pidana

Tindak pidana merupakan suatu istilah yang mengandung suatu pengertian dasar dalam ilmu hukum, sebagai istilah yang dibentuk dengan kesadaran dalam memberikan ciri tertentu pada peristiwa hukum pidana. Tindak pidana mempunyai pengertian yang abstrak dari peristiwa peristiwa yang konkrit dalam lapangan hukum pidana, sehingga tindak pidana haruslah diberikan arti yang bersifat ilmiah dan ditentukan dengan jelas untuk dapat memisahkan dengan istilah yang dipakai sehari-hari dalam kehidupan masyarakat⁸.

Tindak pidana merujuk pada suatu perbuatan yang dilarang oleh hukum dan diancam dengan sanksi pidana. Dalam konteks hukum Islam, istilah ini dikenal dengan sebutan "*jarimah*" atau "*jinayah*". Secara etimologi, kata *jarimah* berasal dari bahasa Arab yang berarti perbuatan yang buruk atau dosa. Menurut para ulama fiqh, *jarimah* adalah perbuatan yang dilarang oleh syariat karena dapat menimbulkan bahaya bagi agama,

⁸ Dr.Fitri Wahyuni, S.H., M.H, *Dasar-Dasar Hukum Pidana di Indonesia*, Ciputat Timur Kota Tangerang Selatan: PT Nusantara Persada Utama, 2017, hlm 35.

jiwa, akal, kehormatan, atau harta benda. Dalam hukum pidana Islam, jarimah dapat dibagi menjadi tiga kategori utama

2) *Deepfake*

Deepfake adalah sebuah bentuk *Artificial Intelligence* (AI) yang menjadi fenomena di era digital pada saat ini, pada beberapa kasus *deepfake* sering digunakan untuk melakukan kejahatan, seperti pemalsuan video maupun audio dengan tujuan merusak reputasi seseorang atau menyebarkan video palsu⁹

Istilah 'deepfake' merupakan istilah kontemporer yang baru dikenal sejak tahun 2017. Oleh karena itu, istilah ini tidak ditemukan secara eksplisit dalam literatur fiqh jinayah klasik. Namun, sejak tahun 2023-2026, istilah *deepfake* telah banyak digunakan dalam kajian-kajian hukum Islam kontemporer sebagai nama fenomenanya, sementara analisis hukumnya tetap didasarkan pada konsep-konsep fiqh seperti kebohongan, penipuan, fitnah, dan jarimah ta'zir.

Deepfake merupakan suatu teknologi yang memanfaatkan kecerdasan buatan (*Artificial Intelligence/AI*) untuk menghasilkan atau memanipulasi konten media, meliputi citra visual, rekaman video, maupun audio, sehingga menampilkan seolah-olah konten autentik, padahal sesungguhnya merupakan rekayasa. Teknologi ini menerapkan teknik machine learning, khususnya *Generative Adversarial Networks (GANs)*, untuk menciptakan media dengan tingkat realisme yang sangat tinggi.

Deepfake dapat diterapkan untuk berbagai tujuan, baik yang bersifat konstruktif maupun destruktif. Namun demikian, penyalahgunaan

⁹ Intan Leliana, Gema Irhamdhika, Achmad Haikal, Rio Septian, Eddy Kusnadi, *Etika Dalam Era Deepfake Bagaimana Menjaga Integritas*, Jurnal Visi Komunikasi, vol 22, no 02, (2023), hlm 9

teknologi tersebut berpotensi menimbulkan dampak negatif, di antaranya adalah penyebaran informasi hoaks, pencemaran nama baik, serta eksploitasi.

3) Hukum Pidana Islam

Hukum pidana Islam merupakan terjemahan dari kata fiqh jinayah. berbagai ketentuan hukum yang mengatur mengenai tindak pidana atau kejahatan (jarimah) beserta sanksi-sanksi hukum ('uqubah) yang dijatuhkan kepada pelakunya. Hal ini dilakukan sebagai bentuk perlindungan terhadap hak-hak Allah SWT dan hak-hak manusia dalam konteks kehidupan bermasyarakat. Ketentuan tersebut dirumuskan oleh para fuqaha (ulama fiqh) yang mukallaf, berdasarkan interpretasi dan pemahaman komprehensif terhadap dalil-dalil hukum yang terperinci bersumber dari Al-Quran dan Hadis.¹⁰

suatu perbuatan dikatakan tindak pidana dapat diformulasikan ke dalam tiga bentuk rukun (perkara), yaitu:

- 1) Rukun *syar'i* (undang-undang), yaitu adanya nash yang melarang suatu perbuatan dengan diancam hukuman kepadanya.
- 2) Rukun *maddi*, yaitu adanya tindakan yang membentuk *jarimah*, baik berupa perbuatan nyata atau tidak.
- 3) Rukun *adabi*, yaitu adanya perbuatan (orang mukallaf) yakni orang yang dapat dimintai pertanggungjawaban terhadap *jarimah* yang dilakukannya.¹¹

E. Kajian Pustaka

Kajian penelitian ini merupakan gambaran terhadap berbagai penelitian yang sudah pernah diteliti peneliti lain yang berkaitan dengan masalah tindak pidana *deepfake*, dan setelah penulis menelusuri beberapa penelitian

¹⁰ Dede Rosyada, *Hukum Islam Dan Pranata Sosial* (Jakarta: Lembaga Studi Islam Dan Kemasyarakatan, 1992), hlm.86

¹¹ Wahbah al-Zuhaili, *Al-Fiqh al-Islami wa Adillatuhu*, Jld. VI. (Damsyik: Dar al-Fikr, 1989), hlm. 215

sebelumnya yang relevan dengan penelitian ini, penulis menemukan beberapa karya tulis ilmiah yang mengkaji tentang permasalahan ini

Pertama penelitian oleh Puteri Nurul Izzah membahas tentang Analisis yuridis Manipulasi gambar *deepfake* pornografi, tujuan dari penelitian tersebut untuk mengetahui konsep pemalsuan gambar *deepfake* serta implementasinya, perbedaan penelitian Puteri Nurul Izzah dengan penelitian ini ialah penelitian terdahulu lebih berfokus pada manipulasi gambar *deepfake* pornografi, sedangkan penelitian ini lebih berfokus tentang bagaimana pendekatan hukum pidana islam dengan undang undang konvensional untuk pencegahan dan pemberantasan pelaku tindak pidana *deepfake*¹²

Kedua Penelitian oleh Sarah Amanda Uly Sijabat membahas tentang perlindungan hukum korban tindak pidana pencemaran nama baik atas penyebaran konten gambar dan vidio pornografi hasil *Artificial intelegence* (AI) *deepfake*, persamaan penelitian Susi Amanda Uly Sijabat sama sama menganalisa bagaimana perlindungan hukum terhadap tindak pidana penyebaran konten gambar yang dihasilkan dari *Artificial intelegence* (AI)¹³

Ketiga Penelitian oleh Meirza Aulia Chairani, Krista Yitawati, Angga Pramoya Pradhana Mengkaji tentang urgensi pengaturan hukum bagi penyalahguna aplikasi *deepfake*, persamaan penelitian mereka dengan penelitian ini sama sama mengkaji ketentuan hukum pidana yang diterapkan pada pelaku penyalahgunaan aplikasi *deepfake*¹⁴

Keempat, penelitian yang dilakukan oleh Antika Setia Dewi dan Dian Alan Setiawan berjudul “*Penegakan Hukum Terhadap Pelaku Deepfake Porn Dihubungkan Hukum Pidana Positif di Indonesia*”. Penelitian tersebut membahas

¹² Puteri Nurul Izzah, *Analisis Yuridis Manipulasi Gambar Deepfake Pornografi* (Surabaya: Universitas Islam Negeri Sunan Ampel, Fakultas Syariah dan Hukum, 2024), hlm. 1–2.

¹³ Sarah Amanda Uly Sijabat dan Diana Lukitasari, “Konten Gambar dan Video Pornografi *Deepfake* Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik,” *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan* 13, no. 2 (2024): 179–194.

¹⁴ Meirza Aulia Chairani, Krista Yitawati, Angga Pramoya Pradhana, *urgensi pengaturan hukum bagi penyalahguna aplikasi Deepfake*, jurnal *Rechtens*, vol. 13 no 1, 2024, hlm 8

penerapan ketentuan hukum pidana positif terhadap pelaku yang menyebarkan konten pornografi berbasis teknologi *deepfake* serta mengidentifikasi berbagai kendala yang dihadapi dalam proses penegakan hukumnya di Indonesia, penelitian terdahulu lebih berfokus pada analisis hukum positif Indonesia, sedangkan penelitian ini juga menelaah permasalahan tersebut dari perspektif hukum pidana Islam.¹⁵

Kelima, penelitian yang dilakukan oleh Isnaini Imroatus dengan judul *“Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia”* membahas aspek perlindungan hukum bagi korban pornografi *deepfake* serta urgensi pembentukan regulasi yang lebih spesifik guna menjamin perlindungan terhadap hak privasi dan kehormatan korban. perbedaannya terletak pada fokus pembahasan, di mana penelitian terdahulu lebih menitikberatkan pada perlindungan hukum bagi korban, sedangkan penelitian ini berorientasi pada analisis tindak pidana, pertanggungjawaban pelaku, serta sanksi yang dapat dikenakan menurut hukum pidana Islam.¹⁶

Keenam, penelitian oleh Natanael Hiskia Mongkau, Herlyanty Y.A. Bawole, dan Altje A. Musa yang berjudul *“Penegakan Hukum Terhadap Penyalahgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Kedalam Gambar atau Video Porno”* mengkaji berbagai bentuk penyalahgunaan teknologi kecerdasan buatan yang digunakan untuk memanipulasi wajah seseorang ke dalam konten pornografi, serta menganalisis instrumen hukum yang dapat diterapkan terhadap pelakunya. Perbedaannya, penelitian terdahulu lebih menekankan pada aspek penegakan hukum positif, sedangkan penelitian ini mengkaji fenomena tersebut melalui pendekatan fiqh

¹⁵ Antika Setia Dewi dan Dian Alan Setiawan, “Penegakan Hukum terhadap Pelaku *Video Deepfake Porn* Dihubungkan dengan Hukum Pidana Positif di Indonesia,” *Bandung Conference Series: Law Studies* 4, no. 1 (2024)

¹⁶ Isnaini Imroatus Solichah, Faizin Sulistio, dan Milda Istiqomah, “Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia,” *International Journal of Multicultural and Multireligious Understanding* 10, no. 1

jinayah dengan menelaah konsep jarimah dan sanksi ta'zir dalam hukum pidana Islam.

Ketujuh, penelitian yang dilakukan oleh Intan Leliana, Gema Irhamdhika, Achmad Haikal, Rio Septian, dan Eddy Kusnadi berjudul “*Etika Dalam Era Deepfake: Bagaimana Menjaga Integritas*”. Penelitian tersebut menyoroti persoalan etika dalam penggunaan teknologi *deepfake* serta pentingnya menjaga integritas informasi di tengah perkembangan teknologi digital yang semakin pesat. penelitian terdahulu menggunakan pendekatan etika komunikasi dalam menganalisis permasalahan tersebut, sedangkan penelitian ini menggunakan pendekatan hukum pidana Islam dan hukum nasional untuk mengkaji kedudukan serta pertanggungjawaban hukum atas penyalahgunaan teknologi *deepfake*.¹⁷

F. Metodologi Penelitian

1) Pendekatan Penelitian

Penelitian ini menerapkan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk mengkaji berbagai aturan hukum yang berkaitan dengan tindak pidana *deepfake* dalam sistem hukum Indonesia. Sementara itu, pendekatan konseptual digunakan untuk menelaah teori, prinsip, dan pandangan para ahli mengenai tindak pidana, jarimah, ta'zir, kejahatan Siber (*Cyber Crime*), serta perkembangan teknologi *deepfake*.

Melalui kedua pendekatan tersebut, penelitian ini bertujuan memperoleh pemahaman yang lebih mendalam mengenai kedudukan hukum dan bentuk pertanggungjawaban terhadap penyalahgunaan teknologi *deepfake* dalam perspektif hukum pidana Islam.

¹⁷ Natanael Hiskia Mongkau, Herlyanty Y. A. Bawole, dan Altje A. Musa, “Penegakan Hukum terhadap Penyalahgunaan Kecerdasan Buatan dengan Cara Memanipulasi Wajah Seseorang ke Dalam Gambar atau Video Porno,” *Lex Administratum* 13, no. 2 (2025): 1–12.

2) Jenis penelitian

Penelitian ini merupakan penelitian hukum normatif atau yuridis normatif. Jenis penelitian ini berorientasi pada kajian terhadap norma, asas, dan ketentuan hukum yang terdapat dalam peraturan perundang-undangan, doktrin hukum, putusan pengadilan, maupun berbagai literatur yang berkaitan dengan topik penelitian.

Penelitian tidak dilakukan melalui pengumpulan data lapangan, tetapi melalui penelaahan berbagai bahan hukum yang relevan dengan tindak pidana *deepfake*. Dengan menggunakan penelitian hukum normatif, penulis berusaha mengkaji dan menganalisis konsep hukum yang dapat digunakan untuk menilai penyalahgunaan teknologi *deepfake* berdasarkan hukum pidana Islam dan hukum positif Indonesia.

3) Sumber Data

Data dalam penelitian ini bersumber dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.

a. Bahan Hukum Primer

Bahan hukum primer merupakan sumber hukum yang memiliki kekuatan mengikat dan menjadi rujukan utama dalam penelitian.

Bahan hukum primer yang digunakan meliputi:

- 1) Al-Qur'an dan Hadis.
- 2) Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Informasi dan Transaksi Elektronik.
- 3) Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi.
- 4) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- 5) Kitab Undang-Undang Hukum Pidana (KUHP).
- 6) Literatur fiqh jinayah yang membahas jarimah dan ta'zir.

b. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan yang berfungsi memberikan penjelasan dan pendukung terhadap bahan hukum primer. Sumber ini terdiri atas:

- 1) Buku-buku yang membahas hukum pidana dan hukum pidana Islam.
 - 2) Artikel dan jurnal ilmiah yang berkaitan dengan deepfake, kejahatan siber, dan fiqh jinayah.
 - 3) Penelitian terdahulu yang memiliki relevansi dengan tema penelitian.
 - 4) Karya ilmiah lain seperti skripsi, tesis, dan disertasi.
- c. Bahan Hukum Tersier

Bahan hukum tersier digunakan sebagai pelengkap untuk membantu memahami bahan hukum primer dan sekunder. Bahan tersebut meliputi:

- 1) Kamus Besar Bahasa Indonesia (KBBI).
- 2) Kamus hukum.
- 3) Ensiklopedia hukum.
- 4) Referensi pendukung lainnya yang relevan dengan penelitian.

4. Teknik Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui studi kepustakaan (*library research*). Metode ini dilakukan dengan cara menelusuri, membaca, memahami, dan menghimpun berbagai sumber hukum yang memiliki relevansi dengan objek penelitian.

Bahan hukum yang di kelompokkan bersumber dari regulasi perundang-undangan, kitab fiqh, buku, jurnal ilmiah, hasil penelitian terdahulu, serta berbagai dokumen yang memiliki keterkaitan dengan tindak pidana *deepfake*. Data yang telah terkumpul Selanjutnya disusun dan diklasifikasikan berdasarkan kategori yang sesuai dengan kebutuhan penelitian guna mempermudah proses analisis data.

5. Objektivitas dan Keabsahan Data

Untuk menjamin objektivitas dan keabsahan data, penelitian ini menggunakan teknik triangulasi sumber. Teknik tersebut dilakukan dengan membandingkan berbagai sumber hukum yang membahas isu yang sama sehingga diperoleh informasi yang lebih akurat dan dapat dipercaya.

Selain itu, penelitian ini hanya menggunakan sumber-sumber yang memiliki kualitas akademik dan dapat dipertanggungjawabkan, seperti peraturan perundang-undangan, kitab fiqh, buku ilmiah, jurnal terakreditasi, dan hasil penelitian yang relevan. Dengan demikian, data yang digunakan diharapkan mampu mendukung analisis secara objektif dan valid.

6. Teknis Analisis Data

Data yang telah terkumpul dianalisis menggunakan metode deskriptif kualitatif. Metode ini dilakukan dengan cara menguraikan, menjelaskan, dan menafsirkan data berdasarkan teori dan konsep yang berkaitan dengan penelitian.

Dalam prosesnya, data dianalisis dengan menghubungkannya pada teori tindak pidana (*jarimah*), teori ta'zir, teori kejahatan siber, dan konsep *deepfake*. Hasil analisis tersebut kemudian digunakan untuk menjawab rumusan masalah serta memperoleh kesimpulan mengenai kedudukan *deepfake* dalam perspektif hukum pidana Islam.

7. Prosedur Penelitian / Sistematika Penelitian

Tahapan penelitian diawali dengan identifikasi masalah yang berkaitan dengan penyalahgunaan teknologi *deepfake*. Setelah itu dilakukan pengumpulan bahan hukum primer, sekunder, dan tersier yang relevan dengan fokus penelitian. Bahan hukum yang telah diperoleh kemudian diklasifikasikan dan dianalisis sesuai dengan kebutuhan penelitian.

Analisis disusun secara sistematis ke dalam beberapa bab. Bab I membahas pendahuluan yang meliputi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, kajian pustaka, dan metodologi penelitian. Bab II berisi landasan teori yang mencakup teori tindak pidana (*jarimah*), teori kejahatan siber, dan konsep *deepfake*. Bab III membahas *deepfake* sebagai tindak pidana melalui kajian kasus serta analisis unsur-unsur *jarimah*. Bab IV memuat analisis hukum pidana Islam terhadap tindak pidana *deepfake* serta kedudukannya sebagai *jarimah ta'zir*. Adapun Bab V berisi kesimpulan dan saran sebagai bagian akhir dari penelitian.

G. Sistematika Pembahasan

Dalam sistematika pada pembahasan skripsi ini terdiri dari empat bab, diantara lain sebagai berikut:

- 1) Bab pertama adalah pendahuluan. Bab ini berisi gambaran umum tentang penelitian yang mencakup latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, tela'ah pustaka, kerangka teori, metode penelitian, dan sistematika penelitian.
- 2) Bab kedua adalah mengenai *deepfake* sebagai tindak pidana, bab ini terdiri dari tiga sub bahasan yaitu konsep *deepfake*, kedua tindak pidana (*jarimah*), ketiga teori kejahatan Siber (Siber Crime).
- 3) Bab ketiga adalah mengenai tinjauan hukum pidana Islam terhadap penyalahgunaan teknologi *deepfake* yang terdiri dari dua sub bahasan yang pertama terkait kasus kasus penyalahgunaan *deepfake* di Aceh, yang kedua terkait bagaimana *deepfake* sebagai tindak pidana *jarimah*
- 4) Bab keempat adalah penutup yang merupakan kesimpulan serta hasil dari penelitian yang telah dikaji.

BAB DUA

PENYALAHGUNAAN DEEPPAKE SEBAGAI TINDAK PIDANA

A. Konsep Deepfake

1. Pengertian *deepfake*

Deepfake merupakan istilah yang terbentuk dari dua gabungan kata *deep learning* dan kata *fake*, Istilah *deep learning* merujuk pada salah satu metode dalam kecerdasan buatan (*artificial intelligence*) yang memungkinkan sistem komputer mempelajari dan mengenali pola dari sejumlah besar data secara otomatis. Sementara itu, kata *fake* berarti palsu atau tiruan. Dengan demikian, secara terminologis, *deepfake* dapat dipahami sebagai teknologi berbasis kecerdasan buatan yang memanfaatkan metode *deep learning* untuk menghasilkan atau memanipulasi konten digital, seperti gambar, video, dan audio, sehingga tampak menyerupai kondisi yang sebenarnya, meskipun konten tersebut merupakan hasil rekayasa atau pemalsuan¹⁸

Dari sisi teknis *deepfake* bekerja dengan menggunakan metode *deep learning* yang memungkinkan sistem komputer menganalisis dan mempelajari karakteristik individu, seperti wajah, suara, ekspresi, serta gerakan tubuh, informasi tersebut kemudian dapat digunakan untuk memproduksi atau menggantikan identitas seseorang dalam media digital lainnya. Tingkat kecanggihan teknologi ini membuat hasil manipulasi yang dihasilkan seringkali sangat sulit untuk dibedakan dari konten asli karena memiliki kemiripan yang sangat tinggi.

¹⁸ Ni Putu Martina Putri, Made Sugi Hartono, I Dewa Gede Herman Yudiawan, “Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence”, Jurnal Pacta Sunt Servanda, Vol. 5, No. (2024), hlm 121

Kemunculan teknologi *deepfake* merupakan salah satu wujud perkembangan pesat dalam bidang kecerdasan buatan yang memberikan berbagai manfaat pada sektor pendidikan, industri hiburan, perfilman, dan komunikasi digital. Namun demikian, di samping manfaat yang ditawarkan, teknologi ini juga berpotensi menimbulkan berbagai persoalan hukum apabila disalahgunakan. Penyalahgunaan *deepfake* dapat digunakan sebagai sarana penyebaran informasi palsu, penipuan, pencemaran nama baik, pelanggaran privasi, hingga pembuatan dan penyebaran konten pornografi yang merugikan pihak lain.

2. Sejarah dan perkembangan *deepfake*

Perkembangan teknologi *deepfake* tidak dapat dipisahkan dari kemajuan kecerdasan buatan (*Artificial Intelligence*) dan *machine learning* yang berkembang pesat pada abad ke-21. Secara konseptual, teknologi yang menjadi dasar *deepfake* telah mulai dikembangkan sejak munculnya penelitian mengenai jaringan saraf tiruan (*artificial neural networks*) dan *deep learning*. Namun, istilah *deepfake* baru dikenal secara luas pada tahun 2017 setelah seorang pengguna platform Reddit menggunakan nama akun "*Deepfakes*" untuk membagikan video hasil manipulasi wajah selebritas ke dalam video lain dengan memanfaatkan teknologi kecerdasan buatan.¹⁹

Pada awalnya, teknologi *deepfake* banyak digunakan dalam industri hiburan, perfilman, dan pengembangan media digital. Teknologi ini dimanfaatkan untuk efek visual dalam film, restorasi gambar bersejarah, hingga pembuatan karakter digital yang menyerupai manusia. Akan tetapi, kemudahan akses terhadap perangkat lunak *deepfake* menyebabkan teknologi tersebut mulai disalahgunakan untuk berbagai tindakan yang bertentangan dengan hukum dan

¹⁹ Robert Chesney dan Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, Vol. 107, No. 6 (2019), hlm. 1758.

etika, seperti pembuatan video pornografi tanpa persetujuan korban, penyebaran berita palsu (*fake news*), penipuan identitas, dan manipulasi informasi politik.²⁰

Di Indonesia, perkembangan *deepfake* mulai mendapatkan perhatian setelah muncul berbagai kasus penyalahgunaan teknologi kecerdasan buatan yang melibatkan manipulasi wajah dan suara tokoh publik. Selain digunakan untuk membuat konten hiburan, teknologi ini juga dimanfaatkan dalam berbagai modus kejahatan Siber, seperti penipuan daring, pencemaran nama baik, serta penyebaran informasi yang menyesatkan masyarakat. Kondisi tersebut menunjukkan bahwa perkembangan teknologi digital tidak hanya membawa manfaat, tetapi juga menimbulkan tantangan baru bagi sistem hukum dalam memberikan perlindungan terhadap hak-hak individu dan kepentingan publik.²¹

Perkembangan teknologi *deepfake* yang semakin canggih diperkirakan akan terus berlangsung seiring meningkatnya kemampuan kecerdasan buatan. Oleh karena itu, diperlukan penguatan regulasi, peningkatan literasi digital masyarakat, serta pengembangan teknologi deteksi *deepfake* guna meminimalisasi dampak negatif yang dapat ditimbulkan oleh penyalahgunaan teknologi tersebut.

3. Cara kerja teknologi *Deepfake*

Teknologi *deepfake* bekerja dengan cara memanfaatkan teknologi kecerdasan buatan (*Artificial intelligence/AI*) yang mampu meniru, mempelajari, mengenali berbagai karakteristik manusia seperti wajah, suara, ekspresi hingga gerakan tubuh. Melalui proses pembelajaran yang kompleks, sistem komputer dapat menghasilkan konten digital baru yang menyerupai individu tertentu dengan tingkat kemiripan yang sangat tinggi. Kemampuan tersebut menjadikan *deepfake* sebagai salah satu bentuk teknologi sintesis media (*synthetic media*)

²⁰ Henry Ajder, Giorgio Patrini, Francesco Cavalli, dan Laurence Cullen, *The State of Deepfakes: Landscape, Threats, and Impact*, Amsterdam: Deeptech Labs, 2019, hlm. 5–10.

²¹ Intan Leliana, Gema Irhamdhika, Achmad Haikal, Rio Septian, dan Eddy Kusnadi, “Etika Dalam Era Deepfake: Bagaimana Menjaga Integritas,” *Jurnal Visi Komunikasi*, Vol. 22, No. 2 (2023), hlm. 147–150.

yang paling berkembang pada era digital saat ini, berikut beberapa cara kerja teknologi *deepfake* :

a. *Artificial intellegence*

Artificial Intelligence (AI) atau kecerdasan buatan merupakan cabang ilmu komputer yang berfokus pada pengembangan sistem yang mampu meniru kemampuan berpikir manusia. Teknologi ini memungkinkan komputer melakukan berbagai tugas yang umumnya memerlukan kecerdasan manusia, seperti mengenali pola, memahami bahasa, mengambil keputusan, dan memecahkan masalah.²²

Dalam teknologi *deepfake*, *AI* berfungsi sebagai fondasi utama yang memungkinkan sistem mengumpulkan, mengolah, dan menganalisis data dalam jumlah besar. Data tersebut kemudian digunakan untuk mempelajari karakteristik seseorang sehingga dapat menghasilkan rekayasa digital yang menyerupai objek aslinya. Semakin banyak data yang tersedia, semakin tinggi pula tingkat akurasi dan realisme hasil *deepfake* yang dihasilkan²³

b. *Machine learning*

Machine Learning merupakan salah satu cabang dari Artificial Intelligence yang memungkinkan sistem komputer belajar secara otomatis dari data tanpa harus diprogram secara rinci untuk setiap tugas yang dilakukan. Melalui metode ini, komputer dapat mengenali pola tertentu dalam data dan menggunakan pola tersebut untuk membuat prediksi atau menghasilkan keluaran baru.²⁴

Dalam proses pembuatan *deepfake*, *machine learning* digunakan untuk mempelajari berbagai karakteristik visual dan audio dari target yang akan

²² Stuart Russell dan Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th Edition (London: Pearson Education, 2021), hlm. 1.

²³ Intan Leliana, Gema Irhamdhika, Achmad Haikal, Rio Septian, dan Eddy Kusnadi, "Etika Dalam Era Deepfake: Bagaimana Menjaga Integritas," *Jurnal Visi Komunikasi*, Vol. 22, No. 2 (2023), hlm. 148.

²⁴ Ethem Alpaydin, *Introduction to Machine Learning*, 4th Edition (Cambridge: MIT Press, 2020), hlm. 3.

dimanipulasi. Sistem akan menganalisis ribuan bahkan jutaan gambar, video, maupun rekaman suara untuk memahami bentuk wajah, ekspresi, gerakan bibir, serta pola suara seseorang. Hasil pembelajaran tersebut kemudian digunakan sebagai dasar untuk menciptakan media sintetis yang menyerupai individu yang menjadi target manipulasi.²⁵

c. *Deep Learning*

Deep Learning merupakan pengembangan lebih lanjut dari *machine learning* yang menggunakan jaringan saraf tiruan (*artificial neural network*) dengan banyak lapisan (*multi-layer neural networks*). Teknologi ini dirancang untuk meniru cara kerja otak manusia dalam mengolah informasi dan mengenali pola yang kompleks.²⁶

Keunggulan *deep learning* ialah terletak pada kemampuannya memproses data dalam jumlah besar dan mengidentifikasi pola yang sulit dikenali melalui metode komputasi biasa. Dalam teknologi *deepfake*, *deep learning* memungkinkan sistem mengenali detail-detail kecil pada wajah seseorang, seperti bentuk mata, hidung, gerakan bibir, ekspresi emosi, hingga intonasi suara. Kemampuan inilah yang menyebabkan hasil manipulasi *deepfake* tampak semakin realistis dan sulit dibedakan dari konten asli.

d. *Generative Adversarial Networks (GANs)*

Salah satu teknologi yang paling berperan dalam perkembangan *deepfake* adalah *Generative Adversarial Networks (GANs)*. Teknologi ini diperkenalkan oleh Ian Goodfellow pada tahun 2014 sebagai metode pembelajaran mesin yang terdiri atas dua jaringan saraf tiruan yang saling berkompetisi, yaitu *generator* dan *discriminator*.

²⁵ Zahra Khanjani, Gabrielle Watson, dan Vandana P. Janeja, "Audio Deepfakes: A Survey," *Frontiers in Big Data*, Vol. 5 (2023), hlm. 4.

²⁶ Ian Goodfellow, Yoshua Bengio, dan Aaron Courville, *Deep Learning* (Cambridge: MIT Press, 2016), hlm. 1.

Generator bertugas menciptakan gambar, video, atau audio palsu berdasarkan data yang telah dipelajari sebelumnya. Sementara itu, *discriminator* bertugas mengevaluasi apakah hasil yang dibuat *generator* merupakan data asli atau data palsu. Kedua sistem tersebut bekerja secara berulang dan saling memperbaiki kemampuannya hingga menghasilkan konten sintetis yang sangat menyerupai data asli.²⁷

Melalui mekanisme tersebut, teknologi *GAN* mampu menghasilkan video dan audio yang memiliki tingkat realisme yang sangat tinggi. Bahkan dalam beberapa kasus, hasil manipulasi *deepfake* sulit dikenali oleh manusia tanpa bantuan perangkat lunak pendeteksi khusus. Oleh karena itu, perkembangan teknologi *GAN* tidak hanya memberikan manfaat bagi dunia industri kreatif, tetapi juga menimbulkan tantangan baru dalam bidang keamanan Siber, perlindungan data pribadi, dan penegakan hukum.²⁸

Berdasarkan uraian tersebut, dapat dipahami bahwa teknologi *deepfake* merupakan hasil perkembangan kecerdasan buatan (*Artificial Intelligence*) yang bekerja melalui serangkaian proses yang saling berkaitan. *Artificial Intelligence* menjadi dasar pengembangan sistem yang mampu meniru kemampuan berpikir manusia, kemudian dikembangkan melalui *Machine Learning* yang memungkinkan sistem belajar dari data secara otomatis. Selanjutnya, *Deep Learning* berperan dalam menganalisis data dengan tingkat kompleksitas yang lebih tinggi melalui jaringan saraf tiruan (*Artificial Neural Network*), sedangkan *Generative Adversarial Networks* (GANs) menjadi algoritma utama yang menghasilkan konten digital berupa gambar, video, maupun audio dengan tingkat kemiripan yang sangat tinggi terhadap objek aslinya. Sinergi dari keempat

²⁷ Ian J. Goodfellow et al., "Generative Adversarial Nets," *Advances in Neural Information Processing Systems*, Vol. 27 (2014), hlm. 2673.

²⁸ Henry Ajder, Giorgio Patrini, Francesco Cavalli, dan Laurence Cullen, *The State of Deepfakes: Landscape, Threats, and Impact* (Amsterdam: Deeptech Labs, 2019), hlm. 8.

teknologi tersebut menjadikan *deepfake* mampu menghasilkan manipulasi digital yang tampak realistis dan sulit dibedakan dari konten asli.

4. Bentuk-bentuk *Deepfake*

Perkembangan teknologi kecerdasan buatan telah melahirkan berbagai bentuk *deepfake* yang mampu memanipulasi identitas seseorang dalam media digital. Manipulasi tersebut dapat berupa perubahan wajah, suara, gambar, maupun penampilan secara langsung (*real-time*) sehingga menghasilkan konten yang tampak autentik. Kemajuan teknologi ini menyebabkan hasil manipulasi semakin sulit dikenali oleh masyarakat umum, sehingga meningkatkan risiko penyalahgunaan untuk berbagai tujuan yang melanggar hukum

a. *Deepfake* dalam bentuk video

Deepfake video merupakan bentuk *deepfake* yang paling banyak ditemukan dalam praktik. Teknologi ini digunakan untuk mengganti wajah seseorang dalam suatu video dengan wajah orang lain sehingga tampak seolah-olah individu tersebut benar-benar melakukan tindakan yang ditampilkan dalam video tersebut. Selain penggantian wajah (*face swapping*), teknologi ini juga mampu memodifikasi gerakan bibir, ekspresi wajah, dan bahasa tubuh agar sesuai dengan narasi yang diinginkan.

Namun demikian, bentuk *deepfake* ini juga sering disalahgunakan untuk membuat video *hoaks*, pencemaran nama baik, propaganda politik, pemerasan, serta pornografi digital yang menggunakan wajah korban tanpa persetujuannya.

b. *Deepfake* dalam bentuk Audio

Deepfake audio merupakan teknologi yang memungkinkan sistem kecerdasan buatan meniru suara seseorang dengan tingkat kemiripan yang sangat tinggi. Teknologi ini bekerja dengan mempelajari karakteristik suara target, seperti intonasi, aksen, ritme bicara, dan pola

pengucapan kata. Setelah proses pembelajaran selesai, sistem dapat menghasilkan suara sintetis yang menyerupai suara asli individu tersebut. Penyalahgunaan *deepfake* audio sering ditemukan dalam berbagai bentuk penipuan digital.

c. *Deepfake* dalam bentuk gambar

Deepfake gambar merupakan bentuk manipulasi visual yang dilakukan terhadap foto atau gambar digital dengan menggunakan teknologi kecerdasan buatan. Manipulasi tersebut dapat berupa penggantian wajah, perubahan ekspresi, penambahan objek tertentu, maupun penggabungan beberapa gambar menjadi satu kesatuan yang tampak nyata.

Dalam berbagai kasus, *deepfake* gambar digunakan untuk menyebarkan informasi palsu, melakukan pencemaran nama baik, serta membuat konten pornografi yang melibatkan wajah korban tanpa izin.

d. *Real-Time Deepfake*

Real-time deepfake merupakan teknologi yang memungkinkan manipulasi wajah dan suara dilakukan secara langsung saat seseorang melakukan komunikasi melalui video konferensi, panggilan video, maupun siaran langsung. Teknologi ini memungkinkan seseorang tampil menggunakan identitas digital yang berbeda dari identitas aslinya.

Kemampuan melakukan manipulasi secara langsung menjadikan *real-time deepfake* sebagai ancaman yang serius dalam sistem keamanan digital. Teknologi ini berpotensi digunakan untuk menyamar sebagai orang lain dalam transaksi keuangan, pertemuan daring, maupun berbagai aktivitas yang memerlukan verifikasi identitas.

5. Dampak penggunaan *deepfake*

Sebagai produk perkembangan kecerdasan buatan, teknologi *deepfake* memiliki dampak yang bersifat ganda. Di satu sisi teknologi ini memberikan manfaat dalam berbagai bidang kehidupan, namun di sisi lain juga dapat

menimbulkan berbagai kerugian apabila digunakan secara tidak bertanggung jawab.

a. Dampak Positif *deepfake*

1. Bidang pendidikan

Deepfake dapat dimanfaatkan sebagai media pembelajaran interaktif yang mampu meningkatkan pemahaman peserta didik. Melalui teknologi ini, tokoh sejarah atau ilmuwan dapat divisualisasikan kembali sehingga proses pembelajaran menjadi lebih menarik dan mudah dipahami

2. Industri perfilman dan Hiburan

Dalam dunia perfilman, *deepfake* digunakan untuk menciptakan efek visual yang lebih realistis serta menghidupkan kembali karakter tertentu yang sulit diwujudkan melalui metode konvensional.

3. Pelestarian Sejarah dan Budaya

Teknologi *deepfake* dapat digunakan untuk merekonstruksi tokoh sejarah dan kebudayaan dalam bentuk digital sehingga dapat dimanfaatkan sebagai sarana edukasi bagi masyarakat

4. Perkembangan Teknologi dan Komunikasi

Deepfake juga berkontribusi dalam pengembangan teknologi komunikasi, khususnya dalam penerjemahan bahasa yang disertai sinkronisasi gerakan bibir sehingga komunikasi antarbahasa menjadi lebih efektif.

b. Dampak Negatif *deepfake*

1. Pornografi *deepfake*

Pembuatan konten pornografi dengan menggunakan wajah seseorang tanpa persetujuannya merupakan salah satu bentuk penyalahgunaan *deepfake* yang paling merugikan korban, baik secara psikologis maupun sosial

2. Pencemaran nama baik

Manipulasi wajah atau suara seseorang dapat menyebabkan korban dianggap melakukan perbuatan tertentu yang sebenarnya tidak pernah dilakukan, sehingga merusak reputasi dan kehormatannya

3. Penipuan Digital

Deepfake sering digunakan sebagai sarana penipuan dengan memanfaatkan identitas atau suara seseorang untuk memperoleh keuntungan ekonomi secara melawan hukum.

4. Pelanggaran Privasi

Penggunaan foto, video, dan suara seseorang tanpa izin dalam pembuatan *deepfake* merupakan bentuk pelanggaran terhadap hak privasi dan perlindungan data pribadi

5. Penyebaran Hoaks

Deepfake memungkinkan terciptanya video atau audio palsu yang tampak meyakinkan sehingga dapat digunakan untuk menyebarkan informasi yang tidak benar dan menyesatkan masyarakat

Berikut tabel dari kasus, bentuk , dan masalah hukum dari penggunaan *deepfake* yang penulis tulis :

No	Kasus	Bentuk Jarimah	Masalah Hukum
1	Pornografi Non-Konsensual Membuat/menyebarkan video/foto manipulasi wajah seseorang ke dalam konten asusila tanpa izin, sering digunakan untuk pemerasan atau penghinaan.	Qadzaf: Menuduh zina tanpa bukti sah, ancaman hadd 80 cambuk. Jarimah terhadap kesusilaan:Menyebarkan hal yang membangkitkan syahwat secara haram. Ta'zir: Karena tidak ada nash spesifik, hukuman ditentukan hakim sesuai tingkat kerusakan.	Kekosongan norma: Kerusakan kehormatan:.

2.	Pencemaran Nama Baik & Fitnah Membuat konten palsu yang seolah-olah seseorang melakukan perbuatan tercela, berbicara hal tidak benar, atau terlibat skandal untuk merusak reputasi.	Buhtan: Fitnah atau tuduhan bohong yang merusak nama baik. Kadzib: Perbuatan berdusta yang dilarang keras dalam Islam. Ta'zir: Sebagai kejahatan yang mengganggu ketertiban sosial.	Kesulitan pembuktian Dampak luas:
3.	Penipuan & Kecurangan Menggunakan deepfake untuk meniru wajah/suara pejabat atau tokoh, meminta transfer uang, atau memanipulasi bukti demi keuntungan finansial.	Al-Ghash & At-Tadlis: Kecurangan dan penipuan yang merugikan orang lain. Melanggar Hifz al-Mal: Merusak prinsip perlindungan harta dalam Maqashid Syariah. Ta'zir: Kategori utama karena tidak termasuk hudud atau qishash.	Penentuan tanggung jawab Kerugian tidak terukur
4.	Pelanggaran Privasi Mengambil dan menggunakan data biometrik (wajah, suara) seseorang tanpa izin untuk kepentingan apapun	Tajassus: Mencari-cari aib atau informasi privat orang lain yang ditutupi. I'tidaa: Perbuatan zalim atau pelanggaran hak asasi individu. Ta'zir: Pelanggaran terhadap martabat dan hak privasi yang dilindungi syariat.	Definisi privasi digital Hak atas identitas.

B. Tindak Pidana (*Jarimah*)

1. Pengertian *Jarimah*

Dalam hukum pidana Islam, tindak pidana dikenal dengan istilah *jarimah* atau *jinayah*. Secara etimologis, kata *jarimah* berasal dari bahasa Arab *jarama-yajrimu* yang berarti melakukan perbuatan dosa, kesalahan, atau tindakan yang tercela. Secara terminologis, para ulama fiqh mendefinisikan jarimah sebagai setiap perbuatan yang dilarang oleh syariat Islam dan diancam dengan hukuman tertentu, baik berupa hudud, qisas-diyat, maupun ta'zir.²⁹

Menurut Abdul Qadir Audah, jarimah adalah segala larangan syariat yang ditetapkan Allah SWT yang pelanggarannya diancam dengan hukuman hudud atau ta'zir. Larangan tersebut bertujuan untuk menjaga kemaslahatan manusia serta melindungi lima unsur pokok yang menjadi tujuan syariat (*maqashid al-syariah*), yaitu agama (*hifz al-din*), jiwa (*hifz al-nafs*), akal (*hifz al-'aql*), keturunan atau kehormatan (*hifz al-nasl/al-'irdh*), dan harta (*hifz al-mal*).³⁰ Dengan demikian, suatu perbuatan dapat dikategorikan sebagai jarimah apabila mengandung unsur pelanggaran terhadap ketentuan syariat dan menimbulkan kemudharatan bagi individu maupun masyarakat.

2. Unsur-unsur *Jarimah*

Suatu perbuatan tidak dapat dikategorikan sebagai jarimah kecuali memenuhi unsur-unsur tertentu. Para ulama fiqh jinayah menjelaskan bahwa terdapat tiga unsur utama yang harus dipenuhi, yaitu:

a. Rukun Syar'i (Unsur Formal)

Rukun syar'i adalah adanya ketentuan syariat yang melarang suatu perbuatan dan menetapkan sanksi terhadap pelakunya. Prinsip ini

²⁹ Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam: Fikih Jinayah* (Jakarta: Sinar Grafika, 2004), hlm. 9.

³⁰ Abdul Qadir Audah, *At-Tasyri' Al-Jina'i Al-Islami Muqaranan bil Qanun Al-Wad'i*, Juz I (Beirut: Muassasah Al-Risalah, 1992), hlm. 66.

didasarkan pada kaidah bahwa tidak ada tindak pidana dan tidak ada hukuman tanpa adanya ketentuan hukum yang mendahuluinya.³¹

Keberadaan rukun syar'i menunjukkan bahwa suatu perbuatan hanya dapat dianggap sebagai jarimah apabila terdapat dalil Al-Qur'an, Hadis, maupun ijtihad ulama yang melarang perbuatan tersebut.

b. Rukun Maddi (Unsur Material)

Rukun maddi merupakan adanya perbuatan nyata yang dilakukan oleh pelaku, baik berupa tindakan aktif maupun pasif yang menimbulkan akibat tertentu. Unsur ini berkaitan dengan manifestasi perbuatan yang dapat diamati dan dibuktikan.³²

Dalam konteks perkembangan teknologi digital, tindakan memanipulasi gambar, video, atau suara seseorang menggunakan teknologi *deepfake* dapat dipandang sebagai bentuk perbuatan nyata yang berpotensi menimbulkan kerugian terhadap korban.

c. Rukun Adabi (Unsur Moral)

Rukun adabi adalah adanya pelaku yang dapat dimintai pertanggungjawaban hukum. Pelaku harus memenuhi syarat sebagai mukallaf, yaitu berakal, baligh, dan memiliki kemampuan memahami akibat dari perbuatannya.³³

Orang yang kehilangan akal, anak yang belum baligh, atau seseorang yang melakukan perbuatan karena paksaan pada prinsipnya tidak dapat dimintai pertanggungjawaban pidana secara penuh menurut hukum Islam.³⁴

3. Klasifikasi Jarimah dalam Hukum Pidana Islam

³¹ Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam: Fikih Jinayah*, hlm. 27–29.

³² Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam: Fikih Jinayah*, hlm. 28–29.

³³ Ibid, hlm. 28.

³⁴ Ibid, hlm. 28–30.

Secara umum, para ulama membagi jarimah menjadi tiga kategori utama berdasarkan jenis sanksinya yaitu:

a. Jarimah Hudud

Jarimah hudud adalah tindak pidana yang bentuk dan hukumannya telah ditentukan secara tegas oleh Al-Qur'an dan Hadis. Hukuman hudud merupakan hak Allah SWT sehingga tidak dapat diubah atau digugurkan oleh manusia.³⁵

Beberapa bentuk jarimah hudud antara lain:

- 1) Zina
- 2) Qadzaf (menuduh zina tanpa bukti)
- 3) Pencurian (sariqah)
- 4) Perampokan (hirabah)
- 5) Minum khamar
- 6) Bughat (pemberontakan)
- 7) Riddah (murtad)³⁶

b. Jarimah Qisas Diyat

Jarimah qisas dan diyat adalah tindak pidana yang berkaitan dengan pelanggaran terhadap jiwa dan anggota tubuh seseorang. Hukuman qisas diberikan berdasarkan prinsip keseimbangan antara perbuatan dan balasan yang diterima pelaku.³⁷

Apabila korban atau ahli waris memberikan maaf, maka hukuman qisas dapat diganti dengan pembayaran diyat sebagai bentuk kompensasi.

c. Jarimah Tazir

Jarimah ta'zir merupakan tindak pidana yang tidak ditentukan secara khusus bentuk maupun hukumannya dalam Al-Qur'an dan Hadis. Penentuan jenis serta berat ringannya hukuman diserahkan kepada

³⁵ Ibid, hlm. 17–18.

³⁶ Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam: Fikih Jinayah*, hlm. 17–18.

³⁷ Ibid. 18–19.

pemerintah atau hakim berdasarkan tingkat kemudharatan yang ditimbulkan.

Menurut Abdul Qadir Audah, ruang lingkup ta'zir sangat luas karena mencakup berbagai bentuk perbuatan yang merugikan masyarakat namun belum diatur secara rinci dalam nash syariat.³⁸ Oleh karena itu, perkembangan bentuk kejahatan baru yang muncul akibat kemajuan teknologi dapat dimasukkan ke dalam kategori jarimah ta'zir.

4. Tujuan Pemidanaan dalam Hukum Pidana Islam

Pemberian sanksi dalam hukum pidana Islam tidak semata-mata bertujuan untuk menghukum pelaku, melainkan juga untuk mewujudkan kemaslahatan masyarakat. Tujuan tersebut meliputi³⁹:

a) Pencegahan (*Az-Zajr*)

Hukuman diberikan agar pelaku maupun masyarakat tidak mengulangi perbuatan yang sama.⁴⁰

b) Pendidikan dan Perbaikan (*Al-Ishlah wa At-Ta'dib*)

Sanksi bertujuan memperbaiki perilaku pelaku sehingga dapat kembali menjadi anggota masyarakat yang baik.⁴¹

c) Perlindungan Masyarakat

Pemidanaan berfungsi melindungi masyarakat dari berbagai tindakan yang dapat mengancam keamanan, ketertiban, dan kehormatan.

d) Menjaga Maqashid al-Syariah

³⁸ Abdul Qadir Audah, *At-Tasyri' Al-Islami Muqaranan bil Qanun Al-Wad'i*, Juz I, hlm. 689.

³⁹ Rahmat Hakim, *Hukum Pidana Islam (Fiqh Jinayah)* (Bandung: CV Pustaka Setia, 2000), hlm. 64–65.

⁴⁰ Ocktoherrinsyah, "Tujuan Pemidanaan dalam Islam," *IN RIGHT: Jurnal Agama dan Hak Azazi Manusia* 1, no. 1 (2011): 43–44.

⁴¹ Rahmat Hakim, *Hukum Pidana Islam (Fiqh Jinayah)*, hlm. 64–65.

Penerapan hukuman bertujuan menjaga lima kebutuhan pokok manusia, yaitu agama, jiwa, akal, kehormatan, dan harta benda.⁴²

Dengan demikian, sistem pemidanaan dalam Islam memiliki orientasi yang lebih luas dibandingkan sekadar pembalasan, yaitu mewujudkan keadilan dan kemaslahatan umum.

C. Teori Kejahatan Siber (*Syber Crime*)

1. Pengertian Kejahatan Siber (*Syber Crime*)

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan manusia. Internet yang pada awalnya diciptakan untuk mempermudah pertukaran informasi kini juga dimanfaatkan sebagai sarana melakukan berbagai tindakan yang bertentangan dengan hukum. Fenomena tersebut dikenal dengan istilah cyber crime atau kejahatan siber.

Secara umum, kejahatan siber merupakan setiap perbuatan melawan hukum yang dilakukan dengan menggunakan komputer, sistem elektronik, jaringan internet, atau perangkat teknologi digital sebagai sarana maupun sasaran kejahatan. Kejahatan ini memiliki karakteristik yang berbeda dengan kejahatan konvensional karena dapat dilakukan tanpa batas wilayah geografis, berlangsung dengan cepat, serta sulit dideteksi identitas pelakunya.⁴³

2. Karakteristik Kejahatan Siber

Kejahatan siber memiliki karakteristik khusus yang membedakannya dari tindak pidana konvensional. Karakteristik tersebut antara lain:

1) Bersifat Lintas Batas (*Borderless*)

⁴² Indra Suhardi, "Hukuman Cambuk di Masa Pandemi Covid-19," *Mahkamah Syar'iyah Aceh*, menjelaskan bahwa tujuan universal hukum Islam adalah meraih kemaslahatan dan menghindari kerusakan, yang diwujudkan melalui perlindungan terhadap agama, jiwa, harta, akal, dan keturunan.

⁴³ Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan* (Jakarta: Kencana, 2014), hlm. 261.

Cyber crime dapat dilakukan dari lokasi mana pun tanpa harus berada di tempat yang sama dengan korban. Pelaku dapat melakukan kejahatan terhadap korban yang berada di negara berbeda hanya dengan memanfaatkan jaringan internet.

2) Menggunakan Teknologi Digital

Media utama yang digunakan dalam cyber crime adalah perangkat elektronik, komputer, telepon pintar, internet, dan berbagai sistem informasi lainnya.

3) Sulit diidentifikasi

Pelaku kejahatan siber sering menggunakan identitas palsu, akun anonim, *virtual private network (VPN)*, maupun berbagai metode lain untuk menyembunyikan identitasnya sehingga menyulitkan proses penegakan hukum.

4) Menimbulkan Kerugian yang luas

Kerugian akibat cyber crime tidak hanya bersifat material, tetapi juga dapat berupa kerusakan reputasi, gangguan psikologis, pelanggaran privasi, hingga ancaman terhadap keamanan negara⁴⁴

Karakteristik tersebut menunjukkan bahwa perkembangan teknologi digital telah menciptakan tantangan baru bagi sistem hukum dalam mengidentifikasi dan menanggulangi berbagai bentuk kejahatan modern.

3. Bentuk-bentuk Kejahatan Siber

Perkembangan teknologi informasi telah melahirkan berbagai bentuk *cyber crime* dengan modus operandi yang semakin kompleks. Beberapa bentuk kejahatan siber yang sering terjadi antara lain:

1) *Hacking*

⁴⁴ Widodo, *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law)* (Yogyakarta: Aswaja Pressindo, 2013), hlm. 35–37.

Hacking merupakan tindakan memasuki sistem komputer atau jaringan tanpa izin pemiliknya dengan tujuan memperoleh akses terhadap data atau informasi tertentu.⁴⁵

2) *Cracking*

Cracking adalah tindakan merusak sistem keamanan komputer dengan tujuan mencuri, mengubah, atau menghancurkan data yang terdapat dalam sistem tersebut.⁴⁶

3) *Phising*

Phishing merupakan bentuk penipuan yang dilakukan dengan cara memperoleh informasi pribadi korban, seperti kata sandi, nomor rekening, maupun data penting lainnya melalui media elektronik.⁴⁷

4) *Identiti Theft*

Identity theft atau pencurian identitas adalah tindakan menggunakan data pribadi milik orang lain tanpa izin untuk memperoleh keuntungan tertentu atau melakukan tindak pidana.⁴⁸

5) *Cyber Pornography*

Cyber pornography merupakan tindakan penyebaran, pembuatan, maupun distribusi konten pornografi melalui media elektronik yang dapat merugikan individu maupun masyarakat.⁴⁹

Dalam praktiknya, penyalahgunaan *deepfake* dapat digunakan untuk berbagai tindak pidana, seperti penipuan, pencemaran nama baik, penyebaran berita bohong (*hoaks*), pemerasan, hingga pembuatan konten pornografi tanpa

⁴⁵ Raden Besse Suryani, "Cyber Crime dalam Perspektif Hukum Pidana Indonesia," *Jurnal Hukum Samudra Keadilan*, Vol. 12, No. 2, 2017, hlm. 235.

⁴⁶ Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Jakarta: Kencana, 2013), hlm. 57.

⁴⁷ fikri Hidayat dan Agus Raharjo, "Perlindungan Hukum terhadap Korban Kejahatan Phishing di Indonesia," *Jurnal Pembangunan Hukum Indonesia*, Vol. 3, No. 1, 2021, hlm. 62.

⁴⁸ Miftahul Jannah, "Perlindungan Data Pribadi terhadap Tindak Pidana Identity Theft di Indonesia," *Jurnal Rechtsvinding*, Vol. 11, No. 2, 2022, hlm. 178.

⁴⁹ Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik* (Jakarta: Rineka Cipta, 2009), hlm. 121

persetujuan korban (*deepfake pornography*). Tindakan tersebut tidak hanya menimbulkan kerugian materiil, tetapi juga berdampak pada rusaknya reputasi, pelanggaran privasi, serta gangguan psikologis korban.

Di Indonesia, belum terdapat pengaturan khusus mengenai tindak pidana *deepfake*. Namun, penyalahgunaannya dapat dijerat melalui ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, maupun peraturan lain yang berkaitan dengan penipuan, pencemaran nama baik, penyebaran informasi elektronik, dan pelanggaran kesusilaan. Oleh karena itu, *deepfake* merupakan salah satu bentuk kejahatan siber yang perlu mendapatkan perhatian khusus karena perkembangan teknologinya terus meningkat dan berpotensi menimbulkan berbagai persoalan hukum di era digital



BAB TIGA

TINJAUAN HUKUM PIDANA ISLAM TERHADAP PENYALAHGUNAAN TEKNOLOGI DEEPPAKE

A. Kasus-kasus penyalahgunaan *deepfake* di Aceh

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) telah membawa perubahan yang sangat besar dalam kehidupan masyarakat, khususnya dalam bidang komunikasi dan penyebaran informasi. Salah satu bentuk perkembangan tersebut adalah teknologi *deepfake*, yaitu teknologi yang mampu memanipulasi wajah, suara, maupun video seseorang sehingga menghasilkan konten digital yang tampak seperti asli.⁵⁰

Di Indonesia, penyalahgunaan teknologi *deepfake* mulai menunjukkan peningkatan dalam beberapa tahun terakhir. Modus kejahatan yang dilakukan tidak hanya terbatas pada penyebaran konten pornografi, tetapi juga berkembang menjadi penipuan daring, pencemaran nama baik, pemerasan, manipulasi informasi politik, hingga penyalahgunaan identitas digital seseorang. Kondisi tersebut juga mulai ditemukan di Provinsi Aceh yang mengalami beberapa kasus penyalahgunaan teknologi berbasis kecerdasan buatan.

Meskipun hingga saat ini belum terdapat perkara yang diputus pengadilan dengan menggunakan istilah "*deepfake*" secara eksplisit, terdapat beberapa peristiwa yang secara substansial memenuhi karakteristik penyalahgunaan teknologi tersebut. Kasus-kasus tersebut menunjukkan bahwa perkembangan teknologi digital telah melahirkan bentuk kejahatan baru yang belum sepenuhnya dapat dijangkau oleh regulasi yang ada. Dengan demikian, analisis hukum yang dilakukan pada bagian selanjutnya akan memiliki dasar faktual yang lebih komprehensif.

⁵⁰ Ni Putu Martina Putri, Made Sugi Hartono, dan I Dewa Gede Herman Yudiawan, "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence," *Jurnal Pacta Sunt Servanda*, Vol. 5, No. 2, 2024

1. Kasus *deepfake* terhadap Relawan kemanusiaan di Aceh

a) Kronologi Kasus

Perkembangan teknologi *Artificial Intelligence* tidak hanya dimanfaatkan untuk melakukan penipuan, tetapi juga digunakan sebagai sarana melakukan pelecehan dan pencemaran nama baik melalui manipulasi identitas digital seseorang. Salah satu kasus yang menjadi perhatian publik di Indonesia adalah penyalahgunaan teknologi *deepfake* yang menimpa seorang kreator konten bernama Afina Syifa. Kasus tersebut menunjukkan bahwa teknologi *deepfake* dapat digunakan untuk merekayasa wajah seseorang ke dalam foto maupun video yang tidak pernah dibuat oleh korban sehingga menimbulkan kerugian yang bersifat materiil maupun immateriil.

Berdasarkan informasi yang beredar di berbagai media massa, wajah Afina Syifa diambil tanpa izin dari akun media sosial miliknya. Foto dan video tersebut kemudian diproses menggunakan aplikasi berbasis *Artificial Intelligence* sehingga menghasilkan konten digital yang memperlihatkan korban seolah-olah melakukan tindakan yang tidak pernah dilakukan dalam kehidupan nyata. Konten hasil manipulasi tersebut kemudian disebarluaskan melalui berbagai platform media sosial dan aplikasi perpesanan sehingga dengan cepat tersebar kepada masyarakat.

Penyebaran konten *deepfake* tersebut mengakibatkan munculnya berbagai komentar negatif, penghinaan, serta penilaian yang merugikan nama baik korban. Sebagian masyarakat mempercayai bahwa konten tersebut merupakan dokumentasi asli sehingga reputasi Afina Syifa mengalami penurunan.

Penyalahgunaan *deepfake* terhadap Afina Syifa lebih mengarah pada pelanggaran terhadap kehormatan, privasi, dan martabat seseorang. Identitas digital korban dijadikan objek manipulasi untuk menghasilkan konten yang bersifat merendahkan, mempermalukan, atau menyesatkan publik. Oleh karena itu, kerugian utama dalam kasus ini bukan hanya kerugian materiil, melainkan

juga kerugian immateriil berupa rusaknya reputasi, hilangnya rasa aman, serta terganggunya kehidupan pribadi korban.⁵¹

Dengan memanfaatkan perangkat lunak *deepfake*, pelaku mampu menciptakan konten yang tampak realistis sehingga masyarakat awam kesulitan membedakan antara konten asli dengan konten hasil rekayasa. Kondisi tersebut semakin meningkatkan risiko terjadinya pencemaran nama baik, penyebaran informasi palsu, serta kekerasan berbasis gender secara daring yang menyasar perempuan sebagai korban.

Berdasarkan uraian tersebut dapat dipahami bahwa kasus Afina Syifa merupakan salah satu bentuk penyalahgunaan teknologi *deepfake* yang berorientasi pada perusakan kehormatan dan reputasi seseorang melalui manipulasi identitas digital. Oleh karena itu, kasus ini perlu dianalisis lebih lanjut untuk mengetahui bentuk penyalahgunaan yang dilakukan pelaku serta pertanggungjawaban hukumnya menurut hukum positif Indonesia dan hukum pidana Islam.

b) Modus Operandi Pelaku

Modus operandi yang digunakan dalam kasus Afina Syifa memperlihatkan pola penyalahgunaan teknologi *deepfake* yang berbeda dengan tindak pidana penipuan. Dalam perkara ini, pelaku memanfaatkan teknologi kecerdasan buatan (*Artificial Intelligence*) untuk membuat foto hasil manipulasi yang menampilkan wajah korban pada gambar yang bersifat vulgar tanpa persetujuan korban. Konten tersebut kemudian dikirimkan secara berulang kepada korban melalui media sosial sebagai bentuk intimidasi dan pelecehan digital. Selain itu, pelaku juga membuat akun palsu yang mencatut identitas ayah korban untuk menghubungi orang-orang terdekatnya sehingga memperluas dampak psikologis yang dialami korban.

⁵¹ Nukilan, "Foto Hasil Rekayasa AI Dikirim untuk Mengancam Relawan Kemanusiaan di Aceh," 30 Mei 2026, diakses 23 Juni 2026.

Tahap pertama yang dilakukan pelaku adalah memperoleh foto-foto Afina Syifa yang tersedia pada media sosial. Foto-foto tersebut kemudian digunakan sebagai bahan untuk menghasilkan gambar manipulatif menggunakan aplikasi berbasis *Artificial Intelligence*.

Tahap berikutnya adalah proses manipulasi digital. Melalui teknologi *deep learning*, wajah korban ditempatkan pada gambar yang tidak pernah dibuat maupun dilakukan oleh korban. Hasil manipulasi tersebut kemudian dikirimkan kepada korban serta disebarluaskan melalui media sosial. Tujuan tindakan tersebut bukan untuk memperoleh keuntungan ekonomi, melainkan untuk memermalukan korban, merusak reputasinya, serta memberikan tekanan psikologis agar korban menghentikan aktivitasnya di ruang digital.

Selain mengirimkan foto hasil manipulasi AI, pelaku juga membuat beberapa akun palsu yang menggunakan identitas ayah korban. Akun-akun tersebut digunakan untuk mengikuti serta menghubungi kerabat dan rekan korban. Modus demikian merupakan bentuk *impersonation* atau penyamaran identitas yang bertujuan memperluas intimidasi terhadap korban.

Berdasarkan rangkaian perbuatan tersebut dapat dipahami bahwa modus operandi dalam kasus Afina Syifa merupakan bentuk penyalahgunaan teknologi *deepfake* yang berorientasi pada pelecehan digital, pencemaran nama baik, dan kekerasan berbasis gender online.

c) Bentuk Penyalahgunaan *Deepfake*

Penyalahgunaan teknologi *deepfake* dalam kasus Afina Syifa digunakan sebagai sarana melakukan pelecehan, intimidasi, dan pembunuhan karakter (*character assassination*). Pelaku memanfaatkan teknologi kecerdasan buatan untuk menghasilkan foto vulgar yang menampilkan wajah korban sehingga seolah-olah gambar tersebut merupakan dokumentasi asli. Akibatnya, korban mengalami kerugian berupa rusaknya nama baik, terganggunya kehidupan pribadi, serta tekanan psikologis akibat penyebaran konten manipulatif.

Apabila ditinjau dari perspektif kejahatan siber, tindakan tersebut merupakan bentuk penyalahgunaan identitas digital (*digital identity abuse*) sekaligus kekerasan berbasis gender online. Korban dipilih karena identitas dan wajahnya digunakan tanpa persetujuan untuk menghasilkan konten yang bersifat seksual. Praktik semacam ini merupakan salah satu bentuk eksploitasi digital yang semakin meningkat seiring berkembangnya teknologi *Artificial Intelligence* dan kemudahan masyarakat mengakses aplikasi pembuat *deepfake*.

Di samping itu, penyebaran gambar yang bersifat vulgar juga berpotensi menimbulkan stigma sosial dan diskriminasi terhadap korban, terutama karena korban adalah seorang perempuan.

2. Kasus Penipuan Menggunakan Manipulasi Wajah dan Suara di Aceh Timur

a) Kronologi Kasus

Salah satu kasus penyalahgunaan teknologi *deepfake* yang menjadi perhatian publik di Aceh adalah kasus yang menimpa Kasi Pammat Direktorat Samapta Polda Aceh, Kopol Sudioanto. Kasus tersebut menunjukkan bahwa perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*) telah dimanfaatkan oleh pelaku kejahatan sebagai sarana untuk melakukan penipuan dengan menggunakan identitas digital orang lain. Berbeda dengan modus penipuan konvensional yang hanya mengandalkan pesan singkat atau panggilan telepon, pelaku dalam kasus ini memanfaatkan teknologi *deepfake* untuk menciptakan identitas digital yang sangat menyerupai korban sehingga lebih mudah memperoleh kepercayaan masyarakat.⁵²

Berdasarkan informasi yang diberitakan media, pelaku mengambil berbagai data pribadi milik Kopol Sudioanto yang tersedia di ruang digital, seperti foto, video, dan rekaman suara. Data tersebut kemudian diolah menggunakan teknologi kecerdasan buatan sehingga menghasilkan konten digital berupa gambar, suara, bahkan panggilan video yang tampak seolah-olah

⁵² Serambi News, "Modus Penipuan Menggunakan Teknologi Deepfake Terjadi di Aceh Timur," 16 Oktober 2025.

berasal dari Kompok Sudioanto sendiri. Hasil manipulasi tersebut selanjutnya digunakan untuk menghubungi keluarga, kerabat, teman, serta masyarakat dengan tujuan memperoleh keuntungan ekonomi secara melawan hukum.⁵³

Modus yang digunakan pelaku sangat beragam. Dalam beberapa kesempatan pelaku menghubungi korban melalui panggilan telepon maupun video sambil mengaku sebagai Kompok Sudioanto. Pelaku kemudian meminta bantuan berupa pinjaman uang dengan alasan terdapat kebutuhan yang mendesak. Tidak hanya itu, pelaku juga menawarkan penjualan kendaraan mewah, seperti mobil Mitsubishi Pajero Sport, dengan harga yang jauh di bawah harga pasar agar calon korban segera melakukan pembayaran. Untuk semakin meyakinkan korban, pelaku turut mengirimkan foto kendaraan beserta dokumen yang menyerupai surat tanda nomor kendaraan (STNK), sehingga seolah-olah transaksi tersebut benar-benar dilakukan oleh Kompok Sudioanto.⁵⁴

Salah satu warga Aceh Timur hampir menjadi korban dari modus tersebut setelah menerima tawaran pembelian mobil dari nomor yang mengatasnamakan Kompok Sudioanto. Korban sempat mempercayai informasi tersebut karena pelaku mampu menampilkan identitas digital yang sangat meyakinkan. Beruntung, sebelum melakukan transaksi, korban melakukan konfirmasi sehingga mengetahui bahwa komunikasi tersebut merupakan bagian dari upaya penipuan berbasis teknologi *deepfake*. Namun demikian, tidak semua korban memiliki kesempatan untuk melakukan verifikasi. Dalam kurun waktu beberapa hari, sejumlah orang dilaporkan telah mentransfer sejumlah uang kepada pelaku sebelum akhirnya menyadari bahwa mereka telah menjadi korban manipulasi identitas digital.

Kasus tersebut menunjukkan bahwa perkembangan teknologi *deepfake* telah mengubah pola kejahatan siber menjadi semakin kompleks. Pelaku tidak lagi sekadar menggunakan identitas palsu atau akun fiktif, tetapi mampu

⁵³ Ibid

⁵⁴ Ibid

merekayasa wajah, suara, maupun karakteristik seseorang sehingga korban percaya bahwa komunikasi dilakukan secara langsung dengan orang yang dikenalnya. Tingginya tingkat kemiripan antara identitas asli dan hasil manipulasi menyebabkan masyarakat awam mengalami kesulitan dalam membedakan konten asli dengan konten hasil rekayasa kecerdasan buatan.

Apabila ditinjau dari karakteristik kejahatan siber, kasus ini memperlihatkan bahwa teknologi *deepfake* telah digunakan sebagai instrumen untuk melakukan penipuan (*fraud*) melalui manipulasi identitas digital. Penyalahgunaan tersebut tidak hanya mengakibatkan kerugian materiil bagi para korban, tetapi juga menimbulkan kerugian immateriil berupa rusaknya reputasi Kompol Sudioanto sebagai aparat penegak hukum. Di samping itu, penyalahgunaan identitas digital juga berpotensi menurunkan tingkat kepercayaan masyarakat terhadap komunikasi elektronik yang selama ini menjadi bagian penting dalam aktivitas sosial dan ekonomi masyarakat.

Berdasarkan uraian tersebut dapat dipahami bahwa kasus yang menimpa Kompol Sudioanto bukan sekadar merupakan tindak pidana penipuan biasa, melainkan telah berkembang menjadi bentuk kejahatan siber modern (*cyber crime*) yang memanfaatkan kecanggihan teknologi kecerdasan buatan.

b) Modus Operandi Pelaku

Kasus penyalahgunaan identitas Kompol Sudioanto menunjukkan bahwa pelaku memanfaatkan perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*) sebagai instrumen utama dalam melakukan tindak pidana penipuan. Modus tersebut menunjukkan bahwa teknologi digital telah mengubah pola kejahatan siber menjadi lebih kompleks dan sulit dideteksi.

Tahap pertama yang dilakukan pelaku adalah mengumpulkan data pribadi milik korban (*data harvesting*). Data tersebut berupa foto, video, rekaman suara, serta informasi mengenai identitas Kompol Sudioanto yang diperoleh dari berbagai sumber yang dapat diakses melalui internet dan media sosial. Kemudahan memperoleh data digital tersebut memungkinkan pelaku memiliki

bahan yang cukup untuk melatih sistem kecerdasan buatan dalam menghasilkan gambar maupun suara sintetis yang memiliki tingkat kemiripan tinggi dengan identitas asli korban. Semakin banyak data yang berhasil dikumpulkan, semakin realistis pula hasil manipulasi yang dihasilkan oleh teknologi *deepfake*.

Setelah memperoleh data yang diperlukan, pelaku melakukan proses manipulasi menggunakan aplikasi berbasis *Artificial Intelligence*. Pada tahap ini, sistem mempelajari karakteristik wajah, ekspresi, pola bicara, serta intonasi suara korban melalui metode *machine learning* dan *deep learning*. Hasil dari proses tersebut berupa identitas digital yang mampu meniru penampilan maupun suara Kopol Sudioanto sehingga sulit dibedakan dengan identitas aslinya oleh masyarakat awam.

Tahap berikutnya adalah penggunaan identitas digital tersebut sebagai sarana melakukan penipuan. Pelaku menghubungi sejumlah orang melalui aplikasi perpesanan maupun panggilan telepon dengan mengatasnamakan Kopol Sudioanto. Dalam beberapa kasus, pelaku menawarkan penjualan kendaraan dengan harga yang jauh di bawah harga pasar atau meminta sejumlah uang dengan alasan tertentu yang bersifat mendesak. Agar korban semakin yakin, pelaku turut mengirimkan foto kendaraan, dokumen pendukung, bahkan menggunakan suara yang menyerupai korban.

Dari sudut pandang kriminologi, modus operandi tersebut memperlihatkan adanya unsur rekayasa sosial (*social engineering*). Pelaku tidak hanya mengandalkan kecanggihan teknologi, tetapi juga memanfaatkan aspek psikologis korban. Kepercayaan masyarakat terhadap figur aparat penegak hukum dijadikan sarana untuk memengaruhi cara berpikir korban sehingga korban terdorong melakukan transaksi tanpa melakukan verifikasi lebih lanjut. Dengan demikian, keberhasilan kejahatan ini tidak hanya bergantung pada kecanggihan teknologi *deepfake*, tetapi juga pada kemampuan pelaku memanipulasi persepsi dan kepercayaan korban.

Selain itu, modus operandi tersebut menunjukkan bahwa penyalahgunaan *deepfake* memiliki karakteristik sebagai kejahatan siber (*cyber crime*). Kejahatan dilakukan melalui sistem elektronik, memanfaatkan jaringan internet, serta dapat dilakukan tanpa adanya pertemuan langsung antara pelaku dan korban. Kondisi ini menyebabkan proses identifikasi pelaku menjadi lebih sulit karena identitas yang digunakan bukan merupakan identitas asli, melainkan identitas digital hasil rekayasa kecerdasan buatan. Akibatnya, aparat penegak hukum menghadapi tantangan yang lebih besar dalam proses penyelidikan maupun pembuktian.

Berdasarkan uraian tersebut dapat dipahami bahwa modus operandi dalam kasus Kompiler Sudioanto dilakukan melalui beberapa tahapan yang saling berkaitan, yaitu pengumpulan data pribadi korban, pembuatan konten *deepfake* menggunakan teknologi kecerdasan buatan, penyamaran identitas digital, serta pemanfaatan identitas tersebut untuk memperoleh keuntungan ekonomi secara melawan hukum.

Pembahasan mengenai modus operandi tersebut menjadi dasar penting untuk menganalisis bentuk penyalahgunaan *deepfake* dalam perspektif hukum pidana. Dengan memahami cara pelaku menjalankan aksinya, dapat diketahui unsur-unsur tindak pidana yang terpenuhi serta hubungan antara penggunaan teknologi *deepfake* dengan perbuatan melawan hukum yang dilakukan.

c) Bentuk Penyalahgunaan *Deepfake*

Kasus penyalahgunaan identitas Kompiler Sudioanto menunjukkan bahwa teknologi *deepfake* telah mengalami pergeseran fungsi dari teknologi yang awalnya dikembangkan untuk kepentingan pendidikan, industri kreatif, dan perfilman menjadi sarana untuk melakukan tindak pidana.

Dalam kasus ini, pelaku tidak hanya menggunakan identitas palsu sebagaimana praktik penipuan konvensional, melainkan menciptakan representasi digital yang menyerupai korban melalui manipulasi wajah, suara, dan identitas visual lainnya. Bentuk penyalahgunaan tersebut merupakan karakteristik

utama *deepfake crime*, yaitu penggunaan teknologi kecerdasan buatan untuk menghasilkan konten digital yang seolah-olah dibuat atau disampaikan oleh seseorang, padahal seluruh konten tersebut merupakan hasil rekayasa algoritma. Kondisi demikian menyebabkan masyarakat semakin sulit membedakan antara informasi yang autentik dengan informasi hasil manipulasi digital⁵⁵

Apabila ditinjau dari perspektif kejahatan siber (*cyber crime*), tindakan pelaku dapat dikategorikan sebagai bentuk manipulasi identitas digital (*digital identity manipulation*). Manipulasi tersebut dilakukan melalui pemanfaatan data biometrik berupa foto, rekaman video, serta suara korban yang kemudian diproses menggunakan teknologi *deep learning*.

Selain merupakan bentuk manipulasi identitas, penggunaan *deepfake* dalam kasus ini juga merupakan bentuk penipuan digital (*cyber fraud*). Pelaku memanfaatkan kepercayaan masyarakat terhadap Kopol Sudioanto sebagai anggota Kepolisian Republik Indonesia untuk memperoleh keuntungan ekonomi. Kepercayaan tersebut dibangun melalui penggunaan wajah, suara, serta identitas korban sehingga calon korban meyakini bahwa komunikasi yang dilakukan benar-benar berasal dari Kopol Sudioanto. Dengan demikian, teknologi *deepfake* berfungsi sebagai alat untuk memperkuat tipu muslihat yang digunakan dalam melakukan penipuan.

Penyalahgunaan teknologi *deepfake* dalam kasus ini tidak hanya mengakibatkan kerugian materiil bagi masyarakat yang menjadi korban penipuan, tetapi juga menimbulkan kerugian immateriil terhadap Kopol Sudioanto sebagai pemilik identitas. Oleh karena itu, dampak penyalahgunaan *deepfake* tidak hanya menyentuh aspek ekonomi, tetapi juga menyangkut kehormatan, privasi, dan keamanan identitas digital seseorang.

Apabila dianalisis berdasarkan hukum positif Indonesia, tindakan pelaku berpotensi memenuhi unsur beberapa tindak pidana. Penyebaran informasi

⁵⁵ Robert Chesney dan Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, Vol. 107, No. 6 (2019), hlm. 1760–1765.

elektronik yang digunakan sebagai sarana penipuan dapat dikenakan ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Di samping itu, penggunaan data biometrik berupa wajah dan suara tanpa persetujuan pemilik data juga bertentangan dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Apabila tindakan tersebut menimbulkan kerugian ekonomi bagi korban, pelaku juga dapat dimintai pertanggungjawaban berdasarkan ketentuan mengenai tindak pidana penipuan dalam Kitab Undang-Undang Hukum Pidana.⁵⁶

B. Analisis Penyalahgunaan *Deepfake* di Aceh dalam Perspektif Hukum Pidana Islam

1. Analisis Kedudukan Deepfake sebagai Jarimah dalam Hukum Pidana Islam

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*) telah melahirkan berbagai bentuk kejahatan baru, salah satunya melalui penyalahgunaan teknologi *deepfake*. Salah satu kasus terjadi terhadap Afina Syifa yang menjadi korban penyalahgunaan teknologi *deepfake* setelah menyampaikan kritik terhadap kondisi sekolah pascabanjir di Aceh.

Korban mengalami intimidasi melalui penyebaran foto tanpa busana hasil rekayasa *deepfake* serta munculnya akun media sosial palsu yang mengatasnamakan ayah korban. Perbuatan tersebut memang tidak mengakibatkan kerugian berupa hilangnya harta benda, namun telah menimbulkan kerugian immateriil berupa rusaknya nama baik, terganggunya kondisi psikologis, hilangnya rasa aman, serta tercemarnya kehormatan dan martabat korban di tengah masyarakat.

⁵⁶ Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Kitab Undang-Undang Hukum Pidana, Pasal 378.

Dalam perspektif hukum pidana Islam, kehormatan (*al-'irdh*) merupakan salah satu hak yang wajib dilindungi. Segala bentuk penghinaan, fitnah, maupun tindakan yang merendahkan martabat seseorang dilarang oleh syariat Islam. Allah SWT berfirman:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا يَجْعَلِ بَعْضُكُمْ عِزًّا لِبَعْضٍ يَكُونُوا لَكُمْ أَعْيُنًا عَلَىٰ آفَاتِهِم بِمَا كَانُوا يَعْمَلُونَ ۚ
 الَّذِينَ يَفْعَلُوا كَلِمَاتٍ ذُنُوبًا يُؤْخَذُ بِهِمْ لِيَكُونَ لَهُمْ عِزٌّ زِينَةً دُنْيَا لَهُمْ فِي آفَاتِهِمْ لَا يُجْنُونَ وَلَا يُنصَرُونَ ۚ
 فَالَّذِينَ هُمْ يُعَذِّبُونَ لَهُمْ لَا يَشْعُرُونَ ۚ وَتِلْكَ الْأَمْثَلُ لِقَوْمٍ يُضِلُّونَ

"Wahai orang-orang yang beriman! Janganlah suatu kaum mengolok-olok kaum yang lain, boleh jadi mereka lebih baik daripada mereka yang mengolok-olok. Dan jangan pula perempuan-perempuan mengolok-olok perempuan lain, boleh jadi yang diperolokkan lebih baik daripada perempuan yang mengolok-olok. Janganlah kamu saling mencela dan jangan saling memanggil dengan gelar-gelar yang buruk...." (QS. Al-Hujurat: 11).

Ayat tersebut menegaskan bahwa Islam memberikan perlindungan terhadap kehormatan dan martabat setiap individu. Oleh karena itu, penyalahgunaan teknologi *deepfake* yang digunakan untuk mempermalukan, mengintimidasi, ataupun mencemarkan nama baik seseorang sebagaimana dialami Afina Syifa merupakan perbuatan yang bertentangan dengan prinsip-prinsip syariat karena menimbulkan kerugian immateriil yang merusak kehormatan korban.

Selain menimbulkan kerugian immateriil, penyalahgunaan *deepfake* juga dapat mengakibatkan kerugian materiil. Hal tersebut tampak dalam kasus yang menimpa Kompol Sudianto, di mana pelaku memanfaatkan foto, video, dan suara korban untuk melakukan penipuan terhadap masyarakat.

Perbuatan tersebut bertentangan dengan prinsip hukum pidana Islam yang melarang setiap orang memperoleh harta melalui cara-cara yang tidak benar. Allah SWT berfirman dalam QS. An-Nisa ayat 29:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَتَّبِعُوا هَٰذَا بَلَاءًا مِّنْ بَيْنِكُمْ هَٰذَا مَلَأُوا لَكُمْ فُجُورًا لَّئِي تَكُونُوا لِلَّذِينَ آمَنُوا سُبُلًا يُخْرِجُوا مِنْهَا أَمْوَالُهُمْ لِتَنكِحُوا الْأَرْوَاحَ الطَّيِّبَاتِ الْمَسْكُونَاتِ ۚ أُولَٰئِكَ حُسْنُ عَمَلِكُمْ ۚ وَالَّذِينَ آمَنُوا يُؤْتُونَ مِمَّا رَزَقْنَاهُمْ يُسْرًا ۚ وَالَّذِينَ آمَنُوا وَتَرَىٰ عَنِ الْفِتَنِ فَضْلُ الْإِسْلَامِ ۚ

"Wahai orang-orang yang beriman! Janganlah kamu saling memakan harta sesamamu dengan jalan yang batil, kecuali dengan jalan perdagangan yang berlaku atas dasar suka sama suka di antara kamu. .." (QS. An-Nisa: 29).

Ayat tersebut menunjukkan bahwa segala bentuk penguasaan harta melalui penipuan, manipulasi, maupun kebohongan merupakan perbuatan yang dilarang dalam Islam. Dalam kasus Kopol Sudioanto, teknologi *deepfake* dijadikan sebagai alat untuk memperoleh keuntungan ekonomi dengan cara menipu masyarakat menggunakan identitas orang lain. Dengan demikian, tindakan tersebut tidak hanya bertentangan dengan hukum positif Indonesia, tetapi juga melanggar prinsip perlindungan harta (*hifzh al-mal*) dalam *maqashid al-syariah*.

Berdasarkan kedua kasus tersebut dapat dipahami bahwa penyalahgunaan teknologi *deepfake* mampu menimbulkan dua bentuk kerugian sekaligus, yaitu kerugian immateriil berupa rusaknya kehormatan, nama baik, dan kondisi psikologis korban, serta kerugian materiil berupa hilangnya harta benda akibat penipuan.

Dari perspektif *fiqh jinayah*, berbagai bentuk penyalahgunaan tersebut menunjukkan adanya kesamaan 'illat dengan perbuatan-perbuatan yang telah dilarang dalam Islam, seperti *al-kadzib* (kebohongan), *buhtan* (fitnah), *at-tadlis* (penipuan), *al-ghasy* (kecurangan), dan setiap perbuatan yang menimbulkan kemudharatan terhadap orang lain. Selain itu, penyalahgunaan *deepfake* juga bertentangan dengan tujuan syariat (*maqashid al-syariah*), khususnya dalam menjaga kehormatan (*hifzh al-'irdh*) dan menjaga harta (*hifzh al-mal*). Oleh karena itu, meskipun teknologi *deepfake* tidak dikenal pada masa klasik dan tidak disebutkan secara eksplisit dalam Al-Qur'an maupun Hadis, substansi penyalahgunaannya memenuhi karakteristik suatu *jarimah* karena mengandung unsur pelanggaran terhadap syariat, dilakukan dengan sengaja, serta menimbulkan kerugian bagi individu maupun masyarakat.

Dengan demikian, penyalahgunaan teknologi *deepfake* dapat dipandang sebagai suatu *jarimah* dalam hukum pidana Islam. Kualifikasi tersebut menjadi dasar untuk menganalisis lebih lanjut apakah perbuatan tersebut telah memenuhi unsur-unsur *jarimah*, bagaimana bentuk pertanggungjawaban pidana pelakunya, serta jenis sanksi yang dapat dijatuhkan menurut perspektif *fiqh jinayah*.

Oleh karena itu, untuk menentukan kedudukan hukum *deepfake* dalam perspektif *fiqh jinayah*, perlu dianalisis terlebih dahulu klasifikasi *jarimah* yang paling sesuai dengan karakteristik perbuatan tersebut. Analisis ini penting untuk mengetahui apakah penyalahgunaan *deepfake* termasuk ke dalam kategori *jarimah hudud*, *jarimah qisas dan diyat*, atau *jarimah ta'zir*.

Demikian pula, penyalahgunaan *deepfake* pada umumnya tidak termasuk ke dalam kategori *jarimah qisas dan diyat*, karena kelompok *jarimah* ini berkaitan dengan tindak pidana yang menyerang jiwa atau anggota badan seseorang sehingga mengakibatkan kematian atau luka fisik yang menjadi dasar pemberlakuan hukuman *qisas* maupun pembayaran *diyat*.

Analisis tersebut didasarkan pada kenyataan bahwa penyalahgunaan *deepfake* merupakan bentuk kejahatan kontemporer yang muncul akibat perkembangan teknologi informasi. Oleh karena itu, berdasarkan pendekatan *fiqh jinayah*, penyalahgunaan *deepfake* lebih tepat dianalisis sebagai *jarimah ta'zir*, karena memberikan ruang bagi pemerintah atau hakim untuk menjatuhkan sanksi yang proporsional sesuai dengan bentuk perbuatan, akibat yang ditimbulkan, serta perkembangan kebutuhan masyarakat modern.

2. Analisis Unsur-Unsur Jarimah pada Tindak Pidana *Deepfake*

Setelah dianalisis bahwa penyalahgunaan teknologi *deepfake* lebih tepat dikualifikasikan sebagai *jarimah ta'zir*, langkah selanjutnya adalah menilai apakah perbuatan tersebut telah memenuhi unsur-unsur *jarimah* dalam perspektif hukum pidana Islam. Analisis ini penting karena suatu perbuatan hanya dapat dipertanggungjawabkan sebagai tindak pidana apabila memenuhi tiga rukun utama dalam *fiqh jinayah*, yaitu *rukun syar'i* (unsur formal), *rukun maddi* (unsur

material), dan *rukun adabi* (unsur moral). Ketiga rukun tersebut menjadi dasar untuk menentukan apakah penyalahgunaan teknologi *deepfake* dapat dikualifikasikan sebagai *jarimah* serta menjadi landasan dalam menetapkan pertanggungjawaban pidana terhadap pelakunya.

a) Rukun Syar'i (Unsur Formal)

Rukun syar'i merupakan adanya ketentuan syariat yang melarang suatu perbuatan. Dalam hukum pidana Islam berlaku asas bahwa tidak ada jarimah dan tidak ada hukuman tanpa adanya dalil yang melarangnya (*la jarīmah wa lā 'uqūbah illā bin nash*). Walaupun Al-Qur'an maupun hadis tidak secara eksplisit menyebut istilah *deepfake*, berbagai bentuk penyalahgunaannya memiliki substansi yang bertentangan dengan prinsip-prinsip syariat Islam.

Penyebaran video palsu, manipulasi identitas seseorang, maupun penggunaan teknologi untuk menipu orang lain merupakan bentuk kebohongan (*al-kadzib*) dan penipuan (*at-tadlis*) yang secara tegas dilarang dalam Islam. Allah SWT berfirman:

يَا أَيُّهَا الَّذِينَ آمَنُوا اتَّقُوا اللَّهَ وَكُونُوا مَعَ الصَّادِقِينَ

"Wahai orang-orang yang beriman, bertakwalah kepada Allah dan hendaklah kamu bersama orang-orang yang benar." (QS. At-Taubah: 119).

Ayat tersebut menunjukkan bahwa Islam mewajibkan kejujuran dan melarang segala bentuk kebohongan, termasuk kebohongan yang dilakukan melalui media digital. Teknologi *deepfake* yang digunakan untuk membuat informasi palsu jelas bertentangan dengan prinsip kejujuran tersebut.

Ayat tersebut menegaskan bahwa kejujuran (*ṣidq*) merupakan salah satu prinsip fundamental dalam ajaran Islam yang harus dijunjung tinggi oleh setiap muslim. Perintah untuk bersama orang-orang yang benar tidak hanya dimaknai sebagai kewajiban berkata jujur, tetapi juga mencakup kewajiban menyampaikan informasi yang sesuai dengan fakta serta menjauhi segala bentuk kebohongan dan manipulasi. Oleh karena itu, meskipun *deepfake* tidak

dikenal pada masa klasik, substansi perbuatannya telah memenuhi unsur pelanggaran terhadap prinsip-prinsip syariat Islam yang melarang kebohongan dan segala bentuk tindakan yang dapat merugikan orang lain.⁵⁷

b) Rukun Maddi (Unsur Material)

Rukun maddi merupakan adanya suatu perbuatan nyata yang dilakukan oleh pelaku sehingga menimbulkan akibat hukum tertentu. Dalam konteks penyalahgunaan *deepfake*, unsur ini terpenuhi karena terdapat tindakan aktif berupa pengambilan data wajah, suara, atau video seseorang, kemudian memanipulasinya menggunakan teknologi *Artificial Intelligence* untuk menghasilkan konten digital palsu.

Dalam perspektif fiqh jinayah, suatu perbuatan yang menimbulkan *adh-dharar* (kemudaratan) terhadap orang lain merupakan perbuatan yang dilarang. Kaidah fiqh menyatakan:

ال ضر يزال

"Kemudaratan harus dihilangkan"⁵⁸

Kaidah tersebut menunjukkan bahwa segala bentuk tindakan yang merugikan hak orang lain wajib dicegah dan diberikan sanksi sesuai tingkat kemudaratanya. Oleh karena itu, penyalahgunaan teknologi *deepfake* yang menimbulkan kerugian terhadap kehormatan, harta, maupun hak pribadi seseorang telah memenuhi unsur material suatu jarimah.

c) Rukun Adabi (Unsur Moral)

Rukun adabi berkaitan dengan kemampuan seseorang untuk dimintai pertanggungjawaban pidana. Dalam hukum Islam, seseorang hanya dapat dikenakan hukuman apabila ia berstatus mukallaf, yaitu telah baligh, berakal, dan melakukan perbuatan tersebut dengan kesadaran serta kehendaknya sendiri.

⁵⁷ Tafsir Al-Misbah, Vol. 5 (Jakarta: Lentera Hati, 2002), penafsiran QS. At-Taubah [9]: 119

⁵⁸ Jalaluddin Abdul Rahman As-Suyuthi, *Al-Asybah wa al-Nazhair* (Beirut: Dar al-Kutub al-'Ilmiyyah, 1998), hlm. 83.

Abdul Qadir Audah menjelaskan bahwa seseorang tidak dapat dipidana apabila kehilangan kemampuan berpikir atau melakukan perbuatan karena paksaan. Sebaliknya, apabila pelaku mengetahui akibat dari perbuatannya dan tetap melaksanakannya secara sukarela, maka ia bertanggung jawab penuh atas jarimah yang dilakukan. Dengan demikian, pelaku penyalahgunaan *deepfake* yang secara sadar membuat maupun menyebarkan konten manipulatif dapat dimintai pertanggungjawaban pidana menurut hukum Islam.

Berdasarkan ketiga unsur tersebut, dapat disimpulkan bahwa penyalahgunaan teknologi *deepfake* telah memenuhi rukun syar'i, karena substansi perbuatannya bertentangan dengan larangan syariat mengenai kebohongan, penipuan, fitnah, dan perbuatan yang menimbulkan kemudharatan. Selanjutnya, unsur rukun maddi juga terpenuhi karena terdapat tindakan nyata berupa manipulasi identitas digital yang mengakibatkan kerugian terhadap korban. Adapun rukun adabi terpenuhi karena pelaku pada umumnya melakukan perbuatannya dengan sengaja dan memiliki kemampuan untuk mempertanggungjawabkan perbuatannya secara hukum

2. *Deepfake* sebagai Jarimah Tazir

Penyalahgunaan teknologi *deepfake* tidak termasuk ke dalam kategori jarimah *hudud* maupun *qisas-diyat* karena tidak terdapat nash Al-Qur'an maupun hadis yang secara tegas mengatur bentuk perbuatan maupun jenis sanksinya. Hal tersebut disebabkan teknologi *deepfake* merupakan hasil perkembangan ilmu pengetahuan modern yang muncul jauh setelah masa pembentukan hukum Islam klasik. Hukum pidana Islam mengenal konsep jarimah ta'zir, yaitu tindak pidana yang bentuk perbuatan maupun hukumannya ditentukan berdasarkan kebijakan

ulil amri atau hakim dengan mempertimbangkan tingkat kemudharatan yang ditimbulkan serta kemaslahatan masyarakat.⁵⁹

Abdul Qadir Audah menyatakan bahwa jarimah *ta'zir* bertujuan memberikan perlindungan terhadap kepentingan umum (*maslahah al-'ammah*) dan mencegah berkembangnya bentuk-bentuk kejahatan baru yang dapat mengganggu ketertiban masyarakat. Oleh karena itu, perkembangan teknologi tidak menghalangi penerapan hukum Islam, sebab setiap bentuk kejahatan baru dapat dikaji berdasarkan persamaan *'illat* dengan perbuatan yang telah dilarang syariat.

Apabila dikaitkan dengan penyalahgunaan *deepfake*, perbuatan pelaku memiliki persamaan *'illat* dengan beberapa bentuk perbuatan yang telah diharamkan dalam Islam. Pertama, penggunaan identitas orang lain untuk memperoleh keuntungan ekonomi merupakan bentuk *at-tadlīs* (penipuan). Dalam fiqh muamalah, *tadlīs* adalah tindakan menyembunyikan fakta atau menciptakan keadaan yang tidak sesuai dengan kenyataan sehingga pihak lain tertipu. Pada kasus Kompol Sudioanto, pelaku memanfaatkan teknologi *Artificial Intelligence* untuk membangun kepercayaan masyarakat dengan mencatut identitas korban. Perbuatan tersebut memiliki tujuan utama memperoleh keuntungan melalui tipu muslihat sehingga secara substansial memenuhi unsur *tadlīs*.

Kedua, penyalahgunaan *deepfake* juga mengandung unsur *al-kadzib* (kebohongan). Pelaku dengan sengaja menciptakan gambar, video, maupun suara yang tidak sesuai dengan kenyataan sehingga masyarakat mempercayai informasi yang sebenarnya tidak pernah terjadi. Kebohongan semacam ini tidak hanya merugikan korban secara materiil, tetapi juga menimbulkan keresahan sosial akibat penyebaran informasi yang menyesatkan. Oleh karena itu, penggunaan teknologi sebagai sarana untuk menyebarkan kebohongan tetap berada dalam

⁵⁹ Abdul Qadir Audah, *At-Tasyri' Al-Jina'i Al-Islami Muqaranan bil Qanun Al-Wad'i*, Juz I (Beirut: Muassasah al-Risalah, 1992), hlm. 79–84; Ahmad Wardi Muslich, *Hukum Pidana Islam* (Jakarta: Sinar Grafika, 2005), hlm. 248–252.

cakupan larangan syariat meskipun medianya mengalami perubahan mengikuti perkembangan zaman.

Selain itu, pada kasus Afina Syifa, penyalahgunaan *deepfake* memiliki kesamaan dengan konsep buhtan (fitnah), yaitu menisbatkan sesuatu yang tidak pernah dilakukan oleh seseorang sehingga merusak kehormatan dan martabatnya. Pelaku merekayasa foto korban menjadi gambar yang bersifat vulgar, kemudian menyebarkannya kepada masyarakat. Akibatnya, korban mengalami tekanan psikologis, pencemaran nama baik, serta kehilangan rasa aman. Dalam perspektif hukum pidana Islam, kehormatan (*'irdh*) merupakan salah satu hak yang wajib dijaga sehingga setiap bentuk perbuatan yang merusaknya termasuk perbuatan yang dilarang.

Di samping mengandung unsur penipuan dan fitnah, penyalahgunaan *deepfake* juga bertentangan dengan kaidah fiqh (*lā ḍarar wa lā ḍirār*), yang berarti tidak boleh menimbulkan bahaya bagi diri sendiri maupun orang lain. Kaidah tersebut menjadi salah satu prinsip utama dalam penetapan hukum Islam, yaitu bahwa setiap perbuatan yang menimbulkan kemudharatan harus dicegah dan pelakunya dapat dikenai sanksi sesuai tingkat kerusakan yang ditimbulkan.

Berdasarkan uraian tersebut, penulis berpendapat bahwa penyalahgunaan teknologi *deepfake* lebih tepat dikualifikasikan sebagai jarimah ta'zir. Klasifikasi ini didasarkan pada tiga pertimbangan utama. Pertama, tidak terdapat ketentuan khusus mengenai *deepfake* dalam nash Al-Qur'an maupun hadis. Kedua, perbuatan tersebut mengandung unsur penipuan, kebohongan, fitnah, serta menimbulkan kemudharatan terhadap masyarakat. Ketiga, penentuan jenis dan berat ringannya hukuman perlu diserahkan kepada pemerintah atau hakim dengan mempertimbangkan perkembangan teknologi, tingkat kesalahan pelaku, dampak yang ditimbulkan, serta kepentingan perlindungan masyarakat. Dengan demikian, penerapan sanksi ta'zir terhadap pelaku penyalahgunaan *deepfake* sejalan dengan tujuan hukum pidana Islam untuk mewujudkan keadilan, memberikan efek jera, serta menjaga kemaslahatan umum.

3. Analisis Unsur Kesengajaan (*Al-Qasd*) dalam Tindak Pidana *Deepfake*

Dalam hukum pidana Islam, unsur kesengajaan (*al-qasd*) merupakan salah satu aspek yang menentukan adanya pertanggungjawaban pidana. Kesengajaan menunjukkan adanya kehendak (*iradah*) dan pengetahuan (*'ilm*) dari pelaku ketika melakukan suatu perbuatan yang dilarang oleh syariat. Dengan kata lain, seseorang hanya dapat dimintai pertanggungjawaban apabila ia mengetahui akibat dari perbuatannya serta secara sadar menghendaki terjadinya akibat tersebut. Oleh karena itu, pembahasan mengenai *al-qasd* menjadi penting dalam menganalisis penyalahgunaan teknologi *deepfake*, mengingat teknologi ini tidak mungkin digunakan tanpa adanya tindakan yang direncanakan dan dilakukan secara sadar oleh pelaku.

Para ulama fiqh menjelaskan bahwa unsur kesengajaan terdiri atas dua komponen utama, yaitu adanya kehendak untuk melakukan suatu perbuatan (*iradah al-fi'l*) dan adanya kehendak terhadap akibat yang ditimbulkan dari perbuatan tersebut (*iradah al-natijah*). Kedua unsur tersebut harus hadir secara bersamaan sehingga suatu perbuatan dapat dikategorikan sebagai jarimah yang dilakukan dengan sengaja (*jarimah al-'amd*). Apabila salah satu unsur tidak terpenuhi, maka bentuk pertanggungjawaban pidananya dapat berbeda sesuai dengan tingkat kesalahan pelaku.

Dalam konteks penyalahgunaan *deepfake*, unsur *al-qasd* tampak sejak tahap awal pelaku melakukan persiapan. Pelaku terlebih dahulu mencari foto, video, atau rekaman suara korban, kemudian mengolah data tersebut menggunakan aplikasi berbasis *Artificial Intelligence* untuk menghasilkan konten manipulatif yang menyerupai identitas asli korban. Setelah konten selesai dibuat, pelaku menyebarkan atau memanfaatkannya dengan tujuan tertentu, seperti memperoleh keuntungan ekonomi, mencemarkan nama baik, melakukan pemerasan, ataupun mempermalukan korban. Rangkaian tindakan tersebut menunjukkan bahwa penyalahgunaan *deepfake* bukanlah perbuatan yang terjadi

secara spontan, melainkan merupakan hasil dari proses yang direncanakan secara sadar dan sistematis.⁶⁰

Pada kasus Kopol Sudioanto, unsur kesengajaan terlihat dari tindakan pelaku yang secara sadar menggunakan identitas korban untuk membangun kepercayaan masyarakat. Pelaku memahami bahwa penggunaan wajah, nama, maupun identitas korban akan meningkatkan keyakinan calon korban sehingga lebih mudah mempercayai informasi yang disampaikan. Tujuan akhirnya adalah memperoleh keuntungan ekonomi melalui penipuan. Dengan demikian, terdapat hubungan yang jelas antara kehendak pelaku, perbuatan yang dilakukan, dan akibat yang ingin dicapai. Hal tersebut menunjukkan terpenuhinya unsur *al-qasd* dalam perspektif fiqh jinayah.

Demikian pula pada kasus Afina Syifa, pelaku secara sengaja memanfaatkan teknologi *deepfake* untuk membuat gambar manipulatif yang bersifat vulgar. Pembuatan konten tersebut memerlukan proses pemilihan foto korban, pengolahan menggunakan teknologi kecerdasan buatan, serta penyebaran kepada publik. Seluruh tindakan tersebut dilakukan secara sadar dengan tujuan merusak kehormatan, mempermalukan korban, dan menimbulkan tekanan psikologis. Oleh karena itu, akibat yang timbul bukanlah sesuatu yang tidak disengaja, melainkan merupakan konsekuensi yang memang dikehendaki oleh pelaku sejak awal. Menurut Abdul Qadir Audah, suatu jarimah dikatakan dilakukan dengan sengaja apabila pelaku mengetahui bahwa perbuatannya dilarang dan tetap melakukannya dengan kehendak bebas tanpa adanya paksaan. Pendapat tersebut menunjukkan bahwa unsur kesengajaan tidak hanya diukur dari niat pelaku, tetapi juga dari proses, alat yang digunakan, dan akibat yang ditimbulkan. Dalam tindak pidana *deepfake*, penggunaan perangkat lunak berbasis *Artificial Intelligence*, pengumpulan data pribadi korban, serta penyebaran konten manipulatif merupakan indikator kuat adanya kesengajaan

⁶⁰ Wahbah Az-Zuhaili, *Al-Fiqh Al-Islami wa Adillatuhu*, Juz VI (Damaskus: Dar al-Fikr, 1989), hlm. 4204–4210.

karena seluruh tahapan tersebut memerlukan pengetahuan, keterampilan, dan perencanaan sebelumnya.

Berdasarkan uraian tersebut, penulis berpendapat bahwa penyalahgunaan teknologi *deepfake* memenuhi unsur kesengajaan (*al-qasd*) dalam hukum pidana Islam. Hal ini didasarkan pada adanya kehendak yang nyata dari pelaku untuk melakukan manipulasi identitas digital, adanya pengetahuan mengenai akibat yang akan timbul, serta adanya tujuan tertentu yang ingin dicapai melalui penyalahgunaan teknologi tersebut. Dengan terpenuhinya unsur *al-qasd*, pelaku tidak hanya bertanggung jawab atas tindakan manipulasi yang dilakukan, tetapi juga atas seluruh kerugian yang ditimbulkan terhadap korban maupun masyarakat.

4. Analisis Pertanggungjawaban Pidana Pelaku *Deepfake* Menurut Fiqh Jinayah

Pertanggungjawaban pidana dalam hukum Islam merupakan konsekuensi hukum yang dibebankan kepada seseorang atas perbuatan yang dilakukan secara sadar dan bertentangan dengan ketentuan syariat. Dalam fiqh jinayah, seseorang tidak serta-merta dikenai hukuman hanya karena telah melakukan suatu perbuatan, tetapi harus terlebih dahulu dibuktikan bahwa pelaku memiliki kecakapan hukum (*ahliyyah*), melakukan perbuatan dengan kehendak sendiri (*ikhtiyar*), memahami akibat dari perbuatannya, serta tidak berada dalam keadaan yang menghapuskan pertanggungjawaban pidana. Oleh karena itu, analisis mengenai pertanggungjawaban pidana menjadi bagian yang sangat penting dalam menentukan apakah pelaku penyalahgunaan teknologi *deepfake* dapat dijatuhi sanksi menurut hukum pidana Islam.

Dalam perspektif fiqh jinayah, syarat utama seseorang dapat dimintai pertanggungjawaban pidana adalah berstatus sebagai mukallaf, yaitu telah baligh, berakal, serta memiliki kemampuan membedakan antara perbuatan yang benar dan yang salah. Apabila syarat tersebut terpenuhi, maka setiap tindakan yang dilakukan atas kehendaknya sendiri akan menimbulkan tanggung jawab hukum. Penyalahgunaan *deepfake* pada umumnya dilakukan oleh orang yang memahami

penggunaan teknologi digital dan secara sadar mengoperasikan perangkat lunak berbasis kecerdasan buatan. Oleh karena itu, pelaku pada umumnya memenuhi syarat sebagai subjek hukum yang dapat dikenai pertanggungjawaban pidana menurut hukum Islam.

Selain memenuhi syarat sebagai *mukallaf*, pertanggungjawaban pidana juga ditentukan oleh adanya hubungan kausal (*sabābiyyah*) antara perbuatan pelaku dengan akibat yang ditimbulkan. Dalam kasus Kumpul Sudianto, kerugian ekonomi yang dialami masyarakat terjadi karena pelaku secara sengaja menggunakan identitas korban sebagai sarana penipuan. Demikian pula pada kasus Afina Syifa, rusaknya nama baik, tekanan psikologis, serta terganggunya kehidupan pribadi korban merupakan akibat langsung dari penyebaran konten *deepfake* yang dibuat oleh pelaku. Dengan demikian, terdapat hubungan sebab akibat yang jelas antara tindakan pelaku dengan kerugian yang dialami korban sehingga pertanggungjawaban pidana tidak dapat dilepaskan dari perbuatan tersebut.

Apabila dianalisis berdasarkan klasifikasi jarimah dalam hukum Islam, penyalahgunaan *deepfake* lebih tepat dikategorikan sebagai jarimah ta'zir. Hal ini disebabkan tidak adanya ketentuan khusus dalam Al-Qur'an maupun hadis yang mengatur bentuk maupun sanksi terhadap penyalahgunaan teknologi *deepfake*. Akan tetapi, substansi perbuatan tersebut memiliki persamaan '*illat*' dengan berbagai bentuk perbuatan yang telah dilarang syariat, seperti penipuan (*at-tadlīs*), kebohongan (*al-kadzib*), fitnah (*buhtān*), kecurangan (*al-ghisy*), serta pengambilan harta orang lain secara batil (*akl al-amwāl bi al-bāṭil*). Oleh karena itu, penetapan sanksinya diserahkan kepada pemerintah atau hakim dengan mempertimbangkan tingkat kesalahan pelaku, akibat yang ditimbulkan, dan kemaslahatan masyarakat.

Konsep *ta'zir* memberikan ruang yang luas bagi *ulil amri* untuk menentukan bentuk sanksi yang paling efektif dalam mencegah berkembangnya kejahatan baru. Dalam konteks penyalahgunaan *deepfake*, bentuk sanksi dapat

berupa pidana penjara, denda, pembayaran ganti rugi kepada korban, penyitaan alat yang digunakan untuk melakukan kejahatan, pembatasan akses terhadap platform digital tertentu, hingga bentuk hukuman edukatif yang bertujuan memberikan efek jera kepada pelaku. Penjatuhan sanksi tersebut harus memperhatikan prinsip proporsionalitas, yaitu keseimbangan antara tingkat kesalahan pelaku dengan kerugian yang ditimbulkan kepada korban maupun masyarakat.

Dengan demikian, penulis berpendapat bahwa pelaku penyalahgunaan teknologi *deepfake* harus dimintai pertanggungjawaban pidana menurut hukum Islam karena telah memenuhi unsur-unsur *jarimah*, dilakukan dengan kesengajaan (*al-qasd*), menimbulkan kemudaratatan terhadap korban, serta bertentangan dengan tujuan syariat (*maqashid al-syari'ah*), prinsip-prinsip keadilan, kemaslahatan, dan perlindungan terhadap hak-hak masyarakat.

5. Analisis Sanksi Ta'zir terhadap Pelaku *Deepfake* Menurut Fiqh Jinayah

Setelah dianalisis bahwa penyalahgunaan teknologi *deepfake* memenuhi unsur-unsur *jarimah* dan lebih tepat dikualifikasikan sebagai *jarimah ta'zir*, maka perlu dikaji bentuk sanksi yang dapat dikenakan kepada pelakunya menurut perspektif *fiqh jinayah*. Analisis mengenai sanksi menjadi penting karena hukum pidana Islam tidak hanya bertujuan memberikan pembalasan kepada pelaku, tetapi juga mewujudkan kemaslahatan, melindungi hak-hak masyarakat, serta mencegah terulangnya tindak pidana yang sama.⁶¹

Dalam hukum pidana Islam, *jarimah ta'zir* merupakan tindak pidana yang jenis maupun sanksinya tidak ditentukan secara tegas dalam Al-Qur'an dan Hadis. Oleh karena itu, kewenangan untuk menentukan bentuk dan berat-ringannya hukuman diberikan kepada *ulil amri* atau hakim dengan mempertimbangkan tingkat kesalahan pelaku, akibat yang ditimbulkan, kondisi korban, serta kemaslahatan masyarakat. Fleksibilitas tersebut menjadikan *ta'zir* mampu

⁶¹ Abdul Qadir Audah, *At-Tasyri' Al-Jina'i Al-Islami Muqaranan bil Qanun Al-Wad'i*, Juz I (Beirut: Muassasah Al-Risalah, 1992), hlm. 609–612.

menjawab berbagai bentuk kejahatan kontemporer, termasuk penyalahgunaan teknologi *deepfake* yang berkembang seiring kemajuan teknologi informasi.

Menurut analisis penulis, karakteristik penyalahgunaan *deepfake* menunjukkan bahwa penjatuhan sanksi tidak dapat disamaratakan. Bentuk sanksi harus disesuaikan dengan tujuan, modus operandi, dan akibat yang ditimbulkan oleh pelaku. Apabila *deepfake* digunakan untuk mencemarkan nama baik, mempermalukan, atau mengintimidasi seseorang sebagaimana kasus yang dialami Afina Syifa, maka hakim dapat menjatuhkan sanksi *ta'zir* yang memberikan efek jera sekaligus memulihkan kehormatan korban. Sebaliknya, apabila *deepfake* digunakan sebagai sarana penipuan sehingga menimbulkan kerugian materiil sebagaimana kasus Kopol Sudianto, maka penjatuhan sanksi harus mempertimbangkan besarnya kerugian ekonomi yang dialami korban serta kewajiban pelaku untuk mengembalikan kerugian tersebut sesuai dengan prinsip keadilan dalam Islam.

Penjatuhan sanksi *ta'zir* terhadap pelaku *deepfake* juga harus memperhatikan tujuan pemidanaan dalam hukum pidana Islam, yaitu *az-zajr* (pencegahan), *al-ishlah wa at-ta'dib* (perbaikan dan pendidikan), serta perlindungan terhadap masyarakat. Sanksi yang dijatuhkan diharapkan tidak hanya memberikan efek jera kepada pelaku, tetapi juga mencegah masyarakat melakukan penyalahgunaan teknologi kecerdasan buatan untuk tujuan yang bertentangan dengan syariat dan hukum positif.

Dalam konteks Indonesia, bentuk sanksi tersebut dapat diwujudkan melalui pidana yang diatur dalam peraturan perundang-undangan, seperti pidana penjara, pidana denda, pembayaran ganti kerugian kepada korban sesuai ketentuan yang berlaku, maupun pidana tambahan berdasarkan putusan pengadilan. Dari perspektif *fiqh jinayah*, bentuk-bentuk pidana tersebut tidak bertentangan dengan konsep *ta'zir* selama ditetapkan oleh pemerintah yang berwenang, bertujuan mewujudkan kemaslahatan, serta memenuhi asas keadilan dan proporsionalitas.

Berdasarkan analisis tersebut, penulis berpendapat bahwa penjatuhan sanksi terhadap pelaku penyalahgunaan teknologi *deepfake* harus didasarkan pada prinsip keadilan, kemanfaatan, dan perlindungan terhadap korban. Fleksibilitas sanksi dalam *jarimah ta'zir* memungkinkan hakim menjatuhkan hukuman yang proporsional sesuai dengan tingkat kesalahan pelaku dan dampak yang ditimbulkan. Oleh karena itu, konsep *ta'zir* merupakan instrumen yang paling relevan untuk memberikan kepastian hukum terhadap penyalahgunaan teknologi *deepfake*, sekaligus mewujudkan tujuan hukum pidana Islam dalam menjaga kehormatan (*hifzh al-'irdh*), harta (*hifzh al-mal*), dan kemaslahatan masyarakat secara keseluruhan.



BAB EMPAT

PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian dan analisis mengenai tindak pidana *deepfake* dalam perspektif hukum pidana Islam, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Penyalahgunaan teknologi *deepfake* merupakan salah satu bentuk kejahatan siber (*cyber crime*) yang memanfaatkan teknologi kecerdasan buatan (*Artificial Intelligence*) untuk memanipulasi gambar, video, maupun suara sehingga menyerupai identitas asli seseorang. Dalam praktiknya, teknologi tersebut telah digunakan untuk berbagai tindak pidana, seperti penipuan, pencemaran nama baik, penyebaran konten pornografi nonkonsensual, pemerasan, penyebaran berita bohong (*hoaks*), serta manipulasi identitas digital. Berdasarkan analisis terhadap kasus Kompol Sudioanto dan Afina Syifa, penyalahgunaan *deepfake* telah menimbulkan kerugian materiil maupun immateriil berupa kerugian ekonomi, kerusakan reputasi, tekanan psikologis, pelanggaran privasi, serta terganggunya ketertiban masyarakat. Oleh karena itu, *deepfake* tidak lagi dipandang sebagai sekadar perkembangan teknologi, melainkan telah berkembang menjadi modus operandi kejahatan siber yang memerlukan penanganan hukum secara serius.
2. Dalam perspektif hukum pidana Islam (*fiqh jinayah*), penyalahgunaan teknologi *deepfake* memenuhi unsur-unsur jarimah karena telah memenuhi rukun syar'i, rukun maddi, dan rukun adabi. Selain itu, perbuatan tersebut dilakukan dengan adanya unsur kesengajaan (*al-qasd*), yaitu adanya kehendak dan pengetahuan pelaku untuk melakukan manipulasi identitas digital serta menghendaki akibat yang ditimbulkan. Penyalahgunaan *deepfake* juga memiliki persamaan *'illat* dengan beberapa

perbuatan yang telah dilarang dalam syariat Islam, seperti *at-tadlīs* (penipuan), *al-kadzib* (kebohongan), *buhtān* (fitnah), dan *al-ghisy* (kecurangan). Meskipun tidak diatur secara eksplisit dalam Al-Qur'an maupun hadis, penyalahgunaan *deepfake* lebih tepat dikualifikasikan sebagai jarimah ta'zir, sehingga penentuan jenis dan bentuk sanksinya menjadi kewenangan *ulil amri* berdasarkan tingkat kemudharatan yang ditimbulkan.

Oleh karena itu, pelaku penyalahgunaan *deepfake* dapat dimintai pertanggungjawaban pidana karena telah melakukan perbuatan yang bertentangan dengan tujuan syariat (*maqashid al-syari'ah*), khususnya dalam menjaga kehormatan (*hifzh al-'irdh*), menjaga harta (*hifzh al-mal*), dan menjaga akal (*hifzh al-'aql*). konsep jarimah ta'zir memberikan dasar hukum yang memadai bagi pemerintah untuk menetapkan kebijakan pemidanaan terhadap kejahatan digital tersebut melalui mekanisme *ijtihad* dan *siyasah syar'iyah*. Dengan demikian, hukum pidana Islam tetap relevan dalam merespons perkembangan teknologi modern karena memiliki karakter yang adaptif terhadap munculnya bentuk-bentuk kejahatan baru.

B. Saran

1. Bagi Pemerintah dan Pembentuk Peraturan Perundang-undangan perlu menyusun regulasi yang secara khusus mengatur penyalahgunaan teknologi *Artificial Intelligence*, khususnya *deepfake*, agar tercipta kepastian hukum dalam proses penegakan hukum. Pengaturan tersebut perlu mengakomodasi berbagai bentuk penyalahgunaan *deepfake*, termasuk penipuan, manipulasi identitas digital, penyebaran konten pornografi nonkonsensual, pencemaran nama baik, dan bentuk kejahatan digital lainnya yang belum diatur secara spesifik dalam peraturan perundang-undangan saat ini.

Pemerintah Aceh diharapkan dapat melakukan pembaruan kebijakan hukum pidana Islam dengan mengkaji kemungkinan pengembangan pengaturan mengenai penyalahgunaan teknologi digital melalui konsep jarimah ta'zir. Mengingat Aceh memiliki kewenangan khusus dalam penyelenggaraan syariat Islam, pengembangan regulasi tersebut diharapkan mampu memberikan perlindungan hukum yang lebih optimal terhadap masyarakat dari berbagai bentuk kejahatan siber yang terus berkembang.

Masyarakat diharapkan lebih bijaksana dalam menggunakan media digital serta meningkatkan literasi digital agar mampu membedakan antara konten asli dan konten hasil manipulasi *deepfake*. Kesadaran masyarakat untuk menjaga data pribadi, tidak mudah mempercayai informasi digital, serta segera melaporkan dugaan penyalahgunaan *deepfake* kepada pihak yang berwenang merupakan langkah penting dalam mencegah berkembangnya kejahatan siber.

2. Penelitian ini masih memiliki keterbatasan karena berfokus pada analisis normatif berdasarkan perspektif fiqh jinayah. Oleh karena itu, penelitian selanjutnya diharapkan dapat mengembangkan kajian mengenai penyalahgunaan *deepfake* melalui pendekatan empiris, perbandingan hukum, maupun analisis terhadap implementasi hukum positif dan hukum pidana Islam dalam penanganan kejahatan berbasis kecerdasan buatan, sehingga dapat memberikan kontribusi yang lebih komprehensif terhadap pengembangan ilmu hukum di Indonesia.

DAFTAR PUSTAKA

- Ajder, Henry, Giorgio Patrini, Francesco Cavalli, dan Laurence Cullen. *The State of Deepfakes: Landscape, Threats, and Impact*. Amsterdam: Deeptrace Labs, 2019.
- Alpaydin, Ethem. *Introduction to Machine Learning*. 4th ed. Cambridge: MIT Press, 2020.
- Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana, 2014.
- As-Suyuthi, Jalaluddin Abdul Rahman. *Al-Asybah wa al-Nazhair*. Beirut: Dar al-Kutub al-'Ilmiyyah, 1998.
- Audah, Abdul Qadir. *At-Tasyri' Al-Jina'i Al-Islami Muqaranan bil Qanun Al-Wad'i*. Juz I. Beirut: Muassasah Al-Risalah, 1992.
- Chairani, Meirza Aulia, Krista Yitawati, dan Angga Pramoya Pradhana. "Urgensi Pengaturan Hukum Bagi Penyalahguna Aplikasi Deepfake." *Jurnal Rechtsens* 13, no. 1 (2024).
- Chesney, Robert, dan Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019).
- Dewi, Antika Setia, dan Dian Alan Setiawan. "Penegakan Hukum Terhadap Pelaku Deepfake Porn Dihubungkan Hukum Pidana Positif di Indonesia." *Bandung Conference Series: Law Studies* 4, no. 1 (2024).
- Fitri Wahyuni. *Dasar-Dasar Hukum Pidana di Indonesia*. Ciputat Timur, Kota Tangerang Selatan: PT Nusantara Persada Utama, 2017.
- Goodfellow, Ian, Yoshua Bengio, dan Aaron Courville. *Deep Learning*. Cambridge: MIT Press, 2016.
- Goodfellow, Ian J., et al. "Generative Adversarial Nets." *Advances in Neural Information Processing Systems* 27 (2014).
- Hidayat, Fikri, dan Agus Raharjo. "Perlindungan Hukum terhadap Korban Kejahatan Phishing di Indonesia." *Jurnal Pembangunan Hukum Indonesia* 3, no. 1 (2021).

- Imroatus, Isnaini. "Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia." *International Journal of Multicultural and Multireligious Understanding* 10, no. 1 (2023).
- Jannah, Miftahul. "Perlindungan Data Pribadi terhadap Tindak Pidana Identity Theft di Indonesia." *Jurnal Rechtsvinding* 11, no. 2 (2022).
- Khanjani, Zahra, Gabrielle Watson, dan Vandana P. Janeja. "Audio Deepfakes: A Survey." *Frontiers in Big Data* 5 (2023).
- Leliana, Intan, Gema Irhamdhika, Achmad Haikal, Rio Septian, dan Eddy Kusnadi. "Etika Dalam Era Deepfake: Bagaimana Menjaga Integritas." *Jurnal Visi Komunikasi* 22, no. 2 (2023).
- Maskun. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana, 2013.
- Media Bangsa. "Deepfake Prabowo Jadi Modus Penipuan Marak Awal 2025." 3 Januari 2026. Diakses 23 Juni 2026.
- Mongkau, Natanael Hiskia, Herlyanty Y. A. Bawole, dan Altje A. Musa. "Penegakan Hukum Terhadap Penyalahgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Kedalam Gambar atau Video Porno." *Jurnal Fakultas Hukum Unsrat* 13, no. 2 (2025).
- Muslich, Ahmad Wardi. *Hukum Pidana Islam*. Jakarta: Sinar Grafika, 2005.
- Ni Putu Martina Putri, Made Sugi Hartono, dan I Dewa Gede Herman Yudiawan. "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence." *Jurnal Pacta Sunt Servanda* 5, no. 2 (2024).
- Nukilan. "Foto Hasil Rekayasa AI Dikirim untuk Mengancam Relawan Kemanusiaan di Aceh." 30 Mei 2026. Diakses 23 Juni 2026.
- OECD. *Computer-Related Crime: Analysis of Legal Policy*. Paris: OECD Publishing, 1986.
- Putu. "Peran Artificial Intelligence (AI) untuk Mendukung Pembelajaran di Masa Pandemi Covid-19." 1, no. 1 (2022).
- Rosyada, Dede. *Hukum Islam dan Pranata Sosial*. Jakarta: Lembaga Studi Islam dan Kemasyarakatan, 1992.

- Russell, Stuart, dan Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th ed. London: Pearson Education, 2021.
- Serambi News. "Modus Penipuan Menggunakan Teknologi Deepfake Terjadi di Aceh Timur." 16 Oktober 2025. Diakses 23 Juni 2026.
- Sunarso, Siswanto. *Hukum Informasi dan Transaksi Elektronik*. Jakarta: Rineka Cipta, 2009.
- Suryani, Raden Besse. "Cyber Crime dalam Perspektif Hukum Pidana Indonesia." *Jurnal Hukum Samudra Keadilan* 12, no. 2 (2017).
- Tri Nurwahid, Sri Amlinawati Muin, dan Rizki Ramadhani. "Deepfake sebagai Kejahatan: Manipulasi AI Audio, Video, dan Gambar dalam Hukum Pidana Indonesia." *Legal Dialogica* 4, no. 2 (2025).
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Widodo. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law)*. Yogyakarta: Aswaja Pressindo, 2013.
- Wahbah al-Zuhaili. *Al-Fiqh al-Islami wa Adillatuhu*. Juz VI. Damaskus: Dar al-Fikr, 1989.

DAFTAR RIWAYAT HIDUP

Nama/NIM : Azzumardi Azra
Tempat/Tgl. Lahir : Palembang 26 September 2003
Jenis Kelamin : Laki-Laki
Pekerjaan : Mahasiswa
Agama : Islam
Kebangsaan/Suku : Gayo
Status : Belum Menikah
Alamat : Jln. Peger Gantung, Dusun Cik,
Desa Kutelintang, Kecamatan Blangkejeren,
Kabupaten Gayo Lues
Orang Tua
Nama Ayah : Abdurrahman, Amd
Nama Ibu : Nuraini, S.P
Alamat : Jln. Peger Gantung, Dusun Cik, Desa
Kutelintang, Kecamatan Blangkejeren,
Kabupaten Gayo Lues
Pendidikan
SD/MI : SD Negeri 3 Blangkejeren
SMP/MTS : Pesantren Modern Shalahuddin Al-Munawwarah
SMA/MAN : Man Negeri 1 Gayo Lues
PT : UIN Ar-Raniry Banda Aceh

Dengan riwayat hidup ini saya buat dengan sebenarnya agar dapat
dipergunakan sebagaimana mestinya

Banda Aceh, 10 Agustus 2026
Penulis



Azzumardi Azra

Lampiran 1 : SK Penetapan Pembimbing Skripsi



**SURAT KEPUTUSAN DEKAN FAKULTAS SYARIAH DAN HUKUM
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH**
Nomor: 92/Un.08/FSH/PP.00.9/1/2026

TENTANG

PENETAPAN PEMBIMBING TUGAS AKHIR MAHASISWA

Menimbang :

- Bahwa untuk kelancaran bimbingan Tugas Akhir pada Fakultas Syariah dan Hukum, maka dipandang perlu menunjukan pembimbing Tugas Akhir tersebut;
- Bahwa yang namanya dalam Surat Keputusan ini dipandang mampu dan cakap serta memenuhi syarat untuk diangkat dalam jabatan sebagai pembimbing Tugas Akhir;
- Bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan keputusan Dekan Fakultas Syariah dan Hukum UIN Ar-Raniry Banda Aceh.

Mengingat :

- Undang-Undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
- Undang-Undang Nomor 14 Tahun 2005 tentang Guru dan Dosen;
- Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi;
- Peraturan Pemerintah Nomor 19 Tahun 2005 tentang Standar Nasional Pendidikan;
- Peraturan Pemerintah RI Nomor 04 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi;
- Peraturan Presiden RI Nomor 64 Tahun 2013 tentang Perubahan Institut Agama Islam Negeri IAIN Ar-Raniry Banda Aceh Menjadi Universitas Islam Negeri;
- Keputusan Menteri Agama 492 Tahun 2003 tentang Pendelegasian Wewenang Pengangkatan, Pemindahan dan Pemberhentian PNS di lingkungan Departemen Agama RI;
- Peraturan Menteri Agama Republik Indonesia Nomor 12 Tahun 2014 tentang Organisasi dan Tata Kerja Universitas Islam Negeri Ar-Raniry Banda Aceh;
- Peraturan Menteri Agama Republik Indonesia Nomor 12 Tahun 2020 tentang Statuta Universitas Islam Negeri Ar-Raniry Banda Aceh;
- Surat Keputusan Rektor UIN Ar-Raniry Nomor 01 Tahun 2015 tentang Pemberi Kuasa dan Pendelegasian Wewenang Kepada Para Dekan dan Direktur Program Pasca Sarjana dalam Lingkungan UIN Ar-Raniry Banda Aceh;

MEMUTUSKAN:

Menetapkan : KEPUTUSAN DEKAN FAKULTAS SYARIAH DAN HUKUM UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH TENTANG BIMBINGAN TUGAS AKHIR

KESATU : Menunjuk Saudara (i):

a. Prof. Dr. Ali Abubakar, M.Ag	Sebagai Pembimbing I
b. Yuhasnibar, M.Ag	Sebagai Pembimbing II

untuk membimbing Tugas Akhir Mahasiswa (i):

Nama : Azzumardi Azra
NIM : 220104076
Prodi : HPI
Judul : Analisis Tindak Pidana Deepfake Dalam Perspektif Hukum Pidana Islam

KEDUA : Kepada pembimbing yang tercantum namanya di atas diberikan honorarium sesuai dengan peraturan perundang-undangan yang berlaku;

KETIGA : Pembiayaan akibat keputusan ini dibebankan pada DIPA UIN Ar-Raniry Tahun 2026;

KEEMPAT : Surat Keputusan ini mulai berlaku sejak tanggal ditetapkan dengan ketentuan bahwa segala sesuatu akan diubah dan diperbaiki kembali sebagaimana mestinya apabila ternyata terdapat kekeliruan dalam keputusan ini.

Kutipan Surat Keputusan ini diberikan kepada yang bersangkutan untuk dilaksanakan sebagaimana mestinya.

Ditetapkan di Banda Aceh
pada tanggal 13 Januari 2026
DEKAN FAKULTAS SYARIAH DAN HUKUM,


KAMARUZZAMAN

Tembusan:

- Rektor UIN Ar-Raniry;
- Ketua Prodi HPI;
- Mahasiswa yang bersangkutan;
- Arsip.