URGENSI PENGATURAN PENYALAHGUNAAN *DEEPFAKE* DI INDONESIA PERSPEKTIF TEORI TANGGUNG JAWAB NEGARA DAN *MAQASHID SYARIAH*

SKRIPSI

Oleh :

Yasmine Nawal Choiry Zavier

220203110011

PROGRAM STUDI HUKUM TATA NEGARA *(SIYASAH)*

FAKULTAS SYARIAH

UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM

MALANG

2026

URGENSI PENGATURAN PENYALAHGUNAAN *DEEPFAKE* DI INDONESIA PERSPEKTIF TEORI TANGGUNG JAWAB NEGARA DAN *MAQASHID SYARIAH*

SKRIPSI

Oleh :

Yasmine Nawal Choiry Zavier

220203110011

PROGRAM STUDI HUKUM TATA NEGARA *(SIYASAH)*

FAKULTAS SYARIAH

UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM

MALANG

2026

PERNYATAAN KEASLIAN SKRIPSI

Demi Allah,

Dengan kesadaran dan rasa tanggung jawab terhadap pengembangan keilmuan, penulis menyatakan bahwa skripsi dengan judul:

URGENSI PENGATURAN PENYALAHGUNAAN *DEEPFAKE* DI INDONESIA PERSPEKTIF TEORI TANGGUNG JAWAB NEGARA DAN *MAQASHID SYARIAH*

Benar-benar merupakan skripsi yang disusun sendiri berdasarkan kaidah penulisan karya ilmiah yang dapat dipertanggungjawabkan. Jika dikemudian hari laporan penelitian skripsi ini merupakan hasil plagiasi karya orang lain baik sebagian maupun keselurutan, maka skripsi sebagai prasyarat mendapat predikat gelar sarjana dinyatakan batal demi hukum.

Malang, 4 Februari 2026

Yas[illegible] Zavier

NIM 220203110011

HALAMAN PERSETUJUAN

Setelah membaca dan mengoreksi skripsi saudara Yasmine Nawal Choiry Zavier NIM: 220203110011 Program Studi Hukum Tata Negara (*Siyasah*) Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan judul :

URGENSI PENGATURAN PENYALAHGUNAAN *DEEPFAKE* DI INDONESIA PERSPEKTIF TEORI TANGGUNG JAWAB NEGARA DAN *MAQASHID SYARIAH*

maka pembimbing menyatakan bahwa skripsi tersebut telah memenuhi syarat-syarat ilmiah untuk diajukan dan diuji oleh Majelis Dewan Penguji.

Mengetahui,	Malang, 4 Februari 2026
Ketua Program Studi	Dosen Pembimbing
Hukum Tata Negara (*Siyasah*)	
Dr. H. Musleh Harry, S.H., M.Hum.	Yayuk Whindari,S.H., M.H.,L.LM.
NIP. 196807101999031002	NIP. 198706202019032013

iii

KEMENTERIAN UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SYARIAH
Jl.Gajayana 50 Malang Telp. (0341) 551354 Fax. (0341)572533

BUKTI KONSULTASI

Nama : Yasmine Nawal Choiry Zavier
NIM : 220203110011
Program Studi : Hukum Tata Negara (*Siyasah*)
Dosen Pembimbing : Yayuk Whindari,S.H., M.H.,L.LM.
Judul Skripsi : **URGENSI PENGATURAN PENYALAHGUNAAN *DEEPFAKE* DI INDONESIA PERSPEKTIF TEORI TANGGUNG JAWAB NEGARA DAN *MAQASHID SYARIAH***

No	Hari/Tanggal	Materi Konsultasi	Paraf
1.	20 Maret 2025	Konsultasi judul	
2.	5 September 2025	Konsultasi latar belakang dan rumusan masalah	
3.	10 September 2025	Konsultasi kerangka teori dan metode penelitian	
4.	29 September 2025	Persetujuan seminar proposal	
5.	27 Oktober 2025	Revisi hasil seminar proposal	
6.	19 November 2025	Konsultasi Bab I dan Bab II	
7.	24 November 2025	ACC revisi Bab I dan Bab II	
8.	5 Januari 2026	Konsultasi Bab III dan Bab IV	
9.	2 Februari 2026	ACC Skripsi Bab III dan Bab IV	
10.	4 Februari 2026	Persetujuan sidang skripsi	

Malang, 4 Februari 2026
Mengetahui,
Ketua Program Studi Hukum Tata Negara (*Siyasah*)

Dr. H. Musleh Harry, S.H., M.Hum
NIP. 196807101999031002

iv

PENGESAHAN SKRIPSI

Dewan Penguji Skripsi saudara Yasmine Nawal Choiry Zavier, NIM 220203110011, mahasiswa Program Studi Hukum Tata Negara (*Siyasah*) Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang, dengan judul:

URGENSI PENGATURAN PENYALAHGUNAAN *DEEPFAKE* DI INDONESIA PERSPEKTIF TEORI TANGGUNG JAWAB NEGARA DAN *MAQASHID SYARIAH*

Telah dinyatakan lulus dengan nilai: 90

Dengan Penguji:

1. Abdul Kadir, S.HI.,M.H.
   NIP. 198207112023211015
   (.....)
   Ketua

2. Yayuk Whindari, S.H.,M.H.,LLM.
   NIP. 198706202019032013
   (.....)
   Sekretaris

3. Dr. M. Aunul Hakim, S.Ag., M.H.
   NIP. 196509192000031001
   (.....)
   Penguji utama

Malang, 02 Maret 2026
Dekan Fakultas Syariah

Dr. Hj. Umi Sumbulah, M.Ag.
NIP. 197108261998032002

MOTTO

كُلُّكُمْ رَاعٍ وَكُلُّكُمْ مَسْئُولٌ عَنْ رَعِيَّتِهِ

"SETIAP KALIAN ADALAH PEMIMPIN, DAN SETIAP KALIAN AKAN DIMINTAI PERTANGGUNGJAWABAN ATAS YANG APA DIPIMPINNYA." (HR. Bukhari, No. 893; Muslim, No 1892)

KATA PENGANTAR

Alhamdulillahirabbil'alamin, ungkapan puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan pertolongan-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul: **"URGENSI PENGATURAN PENYALAHGUNAAN *DEEPFAKE* DI INDONESIA PERSPEKTIF TEORI TANGGUNG JAWAB NEGARA DAN *MAQASHID SYARIAH*"** dengan baik. Shalawat dan salam kita haturkan kepada baginda Rasulullah Muhammad SAW yang telah memberikan uswatun hasanah kepada kita dalam menjalani kehidupan ini secara syar'i. Dengan mengkuti beliau, semoga kita tergolong orang-orang yang beriman dan mendapatkan syafaatnya di hari akhir kiamat. Amin.

Dengan segala pengajaran, bimbingan/ pengarahan, serta bantuan layanan yang telah diberikan, maka dengan segala kerendahan hati penulis menyampaikan ucapan terima kasih yang tiada taranya kepada:

1. Ibu Prof. Dr. Hj. Ilfi Nur Diana, M.Si., CAHRM, CRMP., selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Ibu Prof. Dr. Hj. Umi Sumbulah, M.Ag., selaku Dekan Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Bapak Dr. Musleh Harry, S.H., M.Hum., selaku Ketua Program Studi Hukum Tata Negara (Siyasah) Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang.

4. Bapak Dr. Musleh Harry, S.H., M.Hum selaku dosen wali penulis selama menempuh kuliah di Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang. Terima kasih penulis haturkan kepada beliau yang telah memberikan bimbingan, saran, serta motivasi selama menempuh perkuliahan.
5. Ibu Yayuk Whindari,S.H., M.H.,L.LM. selaku dosen pembimbing penulis yang telah mencurahkan waktu untuk memberikan pengarahan dan motivasi dalam menyelesaikan penulisan skripsi ini.
6. Segenap dosen Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan pembelajaran. Dengan niat yang ikhlas, semoga amal mereka semua menjadi bagian dari ibadah untuk mendapatkan ridha Allah SWT.
7. Kedua orang tua tercinta, Abi Choirudin Wahyu Widodo dan Umi Ery Purwatingsih (almh) atas semua pengorbanan dan jasa beliau berdua sehingga penulis bisa sampai pada titik ini. Terima kasih atas doa-doa yang selalu beliau berdua panjatkan sehingga menjadi kekuatan bagi penulis untuk terus melangkah menggapai tujuan dan cita-cita.
8. Seluruh teman-teman penulis yang selalu membersamai, memotivasi, dan membantu dalam penulisan skripsi ini. Khususnya teman dekat penulis di kampus, yakni: Fadhillatul, Kiki, dan Nuriska.
9. Kepada pihak yang tidak bisa penulis sebutkan satu persatu yang telah membantu dalam proses penulisan mulai dari awal sampai akhir. Terima kasih untuk kalian semua.

Dengan terselesaikannya skripsi ini, harapannya ilmu yang telah penulis peroleh selama kuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang dapat memberikan manfaat bagi agama dan bangsa, serta menjadi amal baik dalam kehidupan dunia dan akhirat. Penulis menyadari bahwa dalam penulisan skripsi ini masih terdapat kekurangan, oleh karena itu, penulis mengharapkan kritik dan saran dari semua pihak untuk perbaikan di masa yang akan datang.

Malang, 4 Februari 2026

Yasmine Nawal Choiry Zavier

NIM 220203110011

PEDOMAN LITERASI

A. Umum

Transliterasi ialah pemindah alihan tulisan Arab ke dalam tulisan Indonesia (Latin), bukan terjemahan bahasa Arab ke dalam bahasa Indonesia. Termasuk dalam kategori ini adalah nama Arab dari bangsa Arab, sedangkan nama Arab dari bangsa selain Arab ditulis sebagaimana ejaan bahasa nasionalnya, atau sebagaimana yang tertulis dalam buku yang menjadi rujukan. Penulisan judul buku dalam catatan kaki (*footnote*) maupun daftar pustaka tetap mengikuti pedoman transliterasi ini. Terdapat berbagai pilihan standart yang dapat digunakan dalam penulisan karya ilmiah, baik pada tingkat nasional, internasional, maupun standart khusus yang diterapkan oleh penerbit tertentu.

Pada penulisan skripsi ini, pedoman transliterasi yang digunakan mengikuti aturan yang diterapkan oleh Fakultas Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang, yang berpedoman pada Ejaan Yang Disenpurnakan (EYD) plus. Pedoman tersebut didasarkan pada Surat Keputusan Bersama (SKB) Kementerian Agama dan Kementerian Pendidikan dan Kebudayaan Republik Indonesia, yang ditetapkan pada 22 Januari 1988 dengan Nomor 158 Tahun 1987 dan Nomor 0534b/U/1987.

Aturan ini juga merujuk pada A Guide Arabic Transliteration yang disusun oleh INIS Fellow pada tahun 1992.

B. Konsonan

Daftar huruf bahasa Arab dan transliterasinya ke dalam huruf Latin dapat dilihat pada halaman berikut:

Huruf Arab	Nama	Huruf Latin	Nama
أ	Alif	Tidak dilambangkan	Tidak dilambangkan
ب	Ba	B	Be
ت	Ta	T	Te
ث	Ṡa	Ṡ	Es (Titik di atas)
ج	Jim	J	Je
ح	Ḥa	Ḥ	Ha (Titik diatas)
خ	Kha	Kh	Ka dan Ha
د	Dal	D	De
ذ	Ż	Ż	Zet (Titik diatas)
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	Es dan Ye

ص	Ṣad	Ṣ	Es (Titik dibawah)
ض	Ḍad	Ḍ	De (Titik dibawah)
ط	Ṭa	Ṭ	Te (Titik dibawah)
ظ	Ẓa	Ẓ	Zet (Titik dibawah)
ع	‘Ain	‘…….	Apostrof terbalik
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qof	Q	Qi
ك	Kaf	K	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha
أ / ء	Hamzah	…….’	Apostrof
ي	Ya	Y	Ye

Hamzah (Á) yang terletak di awal kata mengikuti vokalnya tanpa diberi tanda apa pun. Jika ia terletak di tengah atau di akhir, maka ditulis dengan tanda (’).

C. Vokal

Vokal bahasa Arab, seperti vokal bahasa Indonesia, terdiri atas vokal tunggal atau monoftong dan vokal rangkap atau diftong. Vokal tunggal

bahasa Arab yang lambangnya berupa tanda atau harakat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin	Nama
◌َ	Fathah	A	A
◌ِ	Kasrah	I	I
◌ُ	Dhammah	U	U

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

Tanda	Nama	Huruf Latin	Nama
◌َي	Fathah dan Ya	Ai	A dan I
◌َو	Fathah dan Wau	Au	A dan U

Contoh:

كَيْفَ : kaifa

حَوْلَ : Haula

D. 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
ي / ◌َا	*Fathah* dan *alif* atau *ya*	Ā	a dan garis diatas

ِي	*Kasrah* dan *ya*	Ī	i dan garis diatas
ُو	*Dhammah* dan *wau*	Ū	u dan garis diatas

Contoh:

مَاتَ : māta

رَمَى : ramā

قِيْلَ : qīla

يَمُوْتُ : yamūtu

E. Ta'Marbutha

Terdapat dua transliterasi untuk *ta marbūṭah*, antara lain: *ta marbūṭah* hidup atau mencapai harakat *fatḥah*, *ḍammah* dan *kasrah*, ditransliterasikan menjadi [t]. Sementara *ta marbūṭah* yang mati atau diberi harakat *sukun*, ditransliterasikan dengan [h]. Bilamana sebuah kata berakhiran *ta marbūṭah* diikuti dengan kata sandang *al-* dan kedua kata tersebut dibaca terpisah, sehingga *ta marbūṭah* transliterasinya menjadi ha (h). Contohnya:

رَوْضَةُ الأَطْفَال : *raudah al-atfāl*

المدِيْنَة الفَضِيْلَة : *al-madinah al-fādīlah*

الحِكْمَةُ : *al-hikmah*

F. Syaddah (Tasyid)

Syaddah atau *tasydid* yang dalam sistem tulisan Arab dilambangkan dengan sebuah tanda *tasydid* (ّ), dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda *syaddah*.

Contohnya:

رَبَّنَا : *rabbanā*

نَجَّيْنَا : *najjainā*

الحَقّ : *al-haqq*

الحَجّ : *al-hajj*

عَدُوٌّ : *‘aduwwun*

Jika huruf ì ber-*tasydid* di akhir sebuah kata dan didahului oleh huruf *kasrah* (ِ), maka ia ditransliterasi seperti huruf maddah (Ī).

Contohnya:

عَرَبِيّ : ‘Arabī (bukan ‘Arabiyy atau ‘Araby)

عَلِيّ : ‘Alī (bukan ‘Aliyy atau ‘Aly)

G. Kata Sandang

Kata sandang dalam sistem tulisan Arab dilambangkan dengan huruf (*alif lam ma‘arifah*). Dalam pedoman transliterasi ini, kata sandang ditransliterasi seperti biasa, al-, baik ketika ia diikuti oleh huruf syamsiah maupun huruf qamariah. Kata sandang tidak mengikuti bunyi huruf

langsung yang mengikutinya. Kata sandang ditulis terpisah dari kata yang mengikutinya dan dihubungkan dengan garis mendatar (-). Contohnya:

الشَمْسُ : *al-syamsu (bukan asy-syamsu)*

الزَّلْزَلَة : *al-zalzalah (bukan az-zalzalah)*

الفَلْسَفَة : *al-falsafah*

البِلَادُ : *al-bilādu*

H. 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 dalam tulisan Arab berupa alif. Contohnya:

تَأْمُرُوْنَ : *ta'murūnā*

النَّوْءُ : *al-nau'*

أُمِرْتُ : *umirtu*

I. Penulisan Kata Arab yang Lazim Digunakan dalam Bahasa Indonesia

Kata, istilah atau kalimat Arab yang ditransliterasi adalah kata, istilah atau kalimat yang belum dibakukan dalam Bahasa Indonesia. Kata, istilah atau kalimat yang sudah lazim dan menjadi bagian dari pembendaharaan Bahasa Indonesia, atau sudah sering ditulis dalam tulisan Bahasa Indonesia, tidak lagi ditulis menurut cara transliterasi di atas.

Misalnya kata Al-Qur'an (dari al-Qur'an), Sunnah, khusus dan umum. Namun, bila kata-kata tersebut menjadi bagian dari satu rangkaian teks Arab, maka mereka harus ditransliterasi secara utuh. Contoh:

Fī ẓilāl al-Qur'ān

Al-Sunnah qabl al-tadwīn

Al-'Ibārāt Fī 'Umūm al-Lafẓ lā bi khuṣūṣ al-sabab

J. Lafz Al-Jalālah (الله)

Kata "Allah" didahului partikel semisal huruf *jarr* dan huruf yang lain atau diposisikan sebagai *muḍāf ilaih* (frasa nominal), ditransliterisasikan tanpa huruf hamzah. Contohnya

دِيْنُ الله : dīnullah

Adapun untuk *ta marbūtah* pada akhir kata yang disandarkan pada *lafadz al-jalalāh*, ditransliterasikan dengan huruf [t]. Contohnya:

فِيْ رَحْمَةِ الله : fi rahmatillah

K. Huruf Kapital

Meskipun dalam sistem penulisan Arab tidak terdapat konsep huruf kapital (All Caps), dalam proses transliterasi ke dalam bahasa Indonesia, huruf-huruf tersebut mengikuti aturan penggunaan huruf kapital sesuai dengan pedoman umum Ejaan Bahasa Indonesia (EYD). Penggunaan huruf kapital diterapkan, misalnya, pada huruf pertama nama diri (seperti nama orang, tempat, atau bulan), serta huruf awal pada setiap kalimat. Apabila nama diri diawali dengan kata sandang "al-", maka yang ditulis dengan huruf kapital tetap huruf pertama dari nama diri tersebut, bukan huruf awal

dari kata sandangnya. Namun, jika kata sandang "al-" berada di awal kalimat, maka huruf "A" pada kata tersebut ditulis dengan kapital menjadi "Al-". Aturan ini juga berlaku dalam penulisan judul referensi yang menggunakan kata sandang "al-", baik dalam teks utama maupun dalam daftar pustaka atau catatan referensi seperti CK, DP, CDK, dan DR.

Contohnya:

Wa mā Muḥammadun illā rasul

Syahru Ramaḍān al-lażī unzila fīh al-Qur'ān

Naṣīr al-Dīn al-Ṭūs

Inna awwala baitin wuḍi'a linnāsi lallażī bi Bakkata mubārakan

Abū Naṣr al-Farābī

Al- Munqiż min al-Ḍalāl

Al- Gazāl

DAFTAR ISI

ABSTRAK

Yasmine Nawal Choiry Zavier, 220203110011, 2026. **Urgensi Pengaturan Penyalahgunaan Deepfake di Indonesia Perspektif Teori Tanggung Jawab Negara Dan Maqashid Syariah.** Skripsi, Program Studi Hukum Tata Negara (Siyasah), Fakultas Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing Yayuk Whindari,S.H., M.H.,L.LM.

Kata kunci: *Deepfake*, Konvensi Budapest, Kejahatan Siber, *Maqashid Syariah*, Tanggung Jawab Negara

Teknologi *deepfake* yang berbasis kecerdasan buatan telah berkembang pesat dan menimbulkan ancaman serius terhadap keamanan siber, stabilitas sosial, ekonomi, dan politik di Indonesia. Penyalahgunaan *deepfake* untuk penipuan, disinformasi, pencemaran nama baik, dan konten non-konsensual telah menyebabkan kerugian finansial yang signifikan serta merusak kepercayaan publik. Namun, regulasi nasional Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), belum secara spesifik dan komprehensif mengatur teknologi *deepfake*, sehingga menimbulkan kekosongan hukum dan tantangan dalam penegakan hukum, terutama untuk kasus lintas yurisdiksi.

Penelitian ini bertujuan untuk menganalisis urgensi ratifikasi Konvensi Budapest sebagai instrumen hukum internasional dalam mengatasi penyalahgunaan *deepfake* di Indonesia, dengan pendekatan Teori Tanggung Jawab Negara dan *Maqashid Syariah*. Penelitian menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*), konseptual (*conceptual approach*), dan komparatif (*comparative approach*). Bahan hukum primer meliputi Konvensi Budapest, UUD NRI 1945, UU ITE, UU PDP, dan peraturan perundang-undangan terkait lainnya, serta peraturan di Italia sebagai pembanding. Bahan hukum sekunder dan tersier diperoleh dari literatur ilmiah, jurnal, dan sumber hukum pendukung.

Hasil penelitian menunjukkan bahwa ratifikasi Konvensi Budapest sangat mendesak untuk memperkuat kerangka hukum nasional, meningkatkan kerja sama internasional dalam penanganan bukti elektronik dan ekstradisi, serta memenuhi tanggung jawab negara dalam menjalankan *due diligence* untuk mencegah kejahatan siber lintas batas. Dari perspektif *Maqashid Syariah*, ratifikasi tersebut

sejalan dengan prinsip *ḥifẓ al-dīn* (agama), *ḥifẓ al-nafs* (jiwa), *ḥifẓ al-'aql* (akal), *ḥifẓ al-nasl* (keturunan), dan *ḥifẓ al-māl* (harta) dengan mencegah kemudaratan (*mafsadah*) dan mewujudkan kemaslahatan (*maslahah*) publik. Dengan demikian, ratifikasi Konvensi Budapest merupakan langkah strategis dan kontekstual untuk mengatasi ancaman *deepfake* serta memperkuat perlindungan hukum dan keamanan digital di Indonesia.

ABSTRACT

Yasmine Nawal Choiry Zavier, 220203110011, 2026. **The Urgency of Regulating Deepfake Abuse in Indonesia from the Perspective of State Responsibility Theory and Maqashid Sharia.** Undergraduate Thesis, Constitutional Law Study Program (*Siyasah*), Faculty of Sharia, Maulana Malik Ibrahim State Islamic University of Malang. Supervisor: Yayuk Whindari, S.H., M.H., L.LM.

Keywords: Budapest Convention*, Deepfake*, *Maqashid Syariah*, Cybercrime, State Responsibility

Deepfake technology, based on artificial intelligence, has rapidly evolved and poses serious threats to cybersecurity, social, economic, and political stability in Indonesia. The misuse of deepfake for fraud, disinformation, defamation, and non-consensual content has caused significant financial losses and eroded public trust. However, Indonesia's national regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), do not specifically and comprehensively regulate deepfake technology, resulting in legal gaps and challenges in law enforcement, especially for cross-jurisdictional cases.

This research aims to analyze the urgency of ratifying the Budapest Convention as an international legal instrument in addressing deepfake misuse in Indonesia, using the State Responsibility Theory and Maqashid Syariah perspectives. The research employs normative legal research methods with statutory, conceptual, and comparative approaches. Primary legal materials include the Budapest Convention, the 1945 Constitution, UU ITE, UU PDP, and other related regulations, as well as regulations in Italy for comparison. Secondary and tertiary legal materials were obtained from scientific literature, journals, and other legal sources.

The results indicate that ratifying the Budapest Convention is urgently needed to strengthen the national legal framework, enhance international cooperation in handling electronic evidence and extradition, and fulfill the state's responsibility in exercising *due diligence* to prevent cross-border cybercrime. From the *Maqashid Syariah* perspective, such ratification aligns with the principles of *ḥifẓ al-dīn* (religion), *ḥifẓ al-nafs* (life), *ḥifẓ al-'aql* (intellect), *ḥifẓ al-nasl* (progeny), and *ḥifẓ al-māl* (property) by preventing harm (*mafsadah*) and

realizing public benefit (*maslahah*). Therefore, ratifying the Budapest Convention is a strategic and contextual step to address the *deepfake* threat and strengthen legal protection and digital security in Indonesia.

ملخص

ياسمين نوال شويري زافيير، 220203110011، 2026. الحاجة الملحة لتنظيم إساءة استخدام التزييف العميق في إندونيسيا: وجهات نظر من نظرية مسؤولية الدولة ومقاصد الشريعة. أطروحة برنامج دراسة القانون الدولة، كلية ،الشريعة، جامعة مولانا مالك إبراهيم الإسلامية الحكومية، مالانج المشرف يايوك ويندري، بكالوريوس في القانون ماجستير في القانون، ماجستير في القانون

الكلمات المفتاحية: التزييف العميق، اتفاقية بودابست، الجرائم الإلكترونية، مقاصد الشريعة،مسؤولية الدولة

تطورت تقنية التزييف العميق القائمة على الذكاء الاصطناعي بسرعة وتشكل تهديدًا خطيرًا للأمن السيبراني والاستقرار الاجتماعي والاقتصادي والسياسي في إندونيسيا. أدى إساءة استخدام التزييف العميق في عمليات ،الاحتيال والتضليل والتشهير والمحتوى غير التوافقي إلى خسائر مالية كبيرة وإلحاق الضرر بثقة الجمهور. ومع ذلك وقانون حماية البيانات (ITEقانون) فإن اللوائح الوطنية الإندونيسية، مثل قانون المعلومات والمعاملات الإلكترونية لا تنظم تقنية التزييف العميق بشكل محدد وشامل، مما يخلق فراغًا قانونيًا وتحديات في ،(PDP قانون) الشخصية إنفاذ القانون، خاصة في القضايا التي تتعدى نطاق الاختصاص القضائي

تهدف هذه الدراسة إلى تحليل مدى إلحاحية التصديق على اتفاقية بودابست كصك قانوني دولي لمعالجة إساءة استخدام التزييف العميق في إندونيسيا، باستخدام نهج مسؤولية الدولة ونهج مقاصد الشريعة. تستخدم الدراسة طريقة البحث القانوني المعياري مع نهج قانوني ونهج مفاهيمي ونهج مقارن. وتشمل المواد القانونية الأولية اتفاقية بودابست، ودستور جمهورية إندونيسيا لعام 1945، وقانون المعلومات والمعاملات الإلكترونية، وقانون حماية .البيانات الشخصية، والقوانين واللوائح الأخرى ذات الصلة، بالإضافة إلى اللوائح المعمول بها في إيطاليا للمقارنة .أما المواد القانونية الثانوية والثالثية فهي مستمدة من الأدبيات العلمية والمجلات والمصادر القانونية الداعمة

تشير نتائج الدراسة إلى أن التصديق على اتفاقية بودابست أمر ملحّ لتعزيز الإطار القانوني الوطني،وتقوية التعاون

الدولي في التعامل مع الأدلة الإلكترونية وتسليم المجرمين، والوفاء بمسؤولية الدولة في بذل العناية الواجبة لمنع الجرائم الإلكترونية العابرة للحدود. من منظور مقاصد الشريعة، يتماشى التصديق مع مبادئ حفظ الدين وحفظ النفس .حفظ العقل، وحفظ النسل، وحفظ المال من خلال منع الضرر (المفسدة) وتحقيق المنفعة العامة (المصلحة) وبالتالي، فإن التصديق على اتفاقية بودابست هو خطوة استراتيجية وسياقية لمواجهة تهديد التزييف العميق وتعزيز .الحماية القانونية والأمن الرقمي في إندونيسيا

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa perubahan yang sangat signifikan dalam kehidupan sosial, ekonomi, budaya, bahkan hukum. Salah satu produk dari kemajuan teknologi yang saat ini menjadi sorotan global adalah kecerdasan buatan *(artificial intelligence/AI),* yang mampu menciptakan simulasi realitas dengan tingkat presisi yang sangat tinggi. Salah satu manifestasi paling mencolok dari *AI* dalam ranah multimedia adalah teknologi *deepfake*, yakni manipulasi citra atau suara digital yang menyerupai individu asli secara meyakinkan. Teknologi ini dapat digunakan untuk berbagai tujuan positif, misalnya dalam bidang perfilman, pelatihan, dan simulasi pendidikan,[1] namun, di sisi lain, teknologi ini juga berpotensi besar disalahgunakan untuk tindakan kejahatan siber, pencemaran nama baik, penipuan, hingga penyebaran konten pornografi non-konsensual.

Pada era digital yang semakin maju, teknologi kecerdasan buatan *(AI)* memungkinkan penciptaan konten sintetis yang sangat realistis dikenal sebagai *deepfake* baik berupa video, suara, maupun gambar, di Indonesia

[1] Anti Mutmainnah dkk., "Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital," *UPGRADE : Jurnal Pendidikan Teknologi Informasi* 1, no. 2 (2024): 67–72, https://doi.org/10.30812/upgrade.v1i2.3702.

fenomena ini bukan lagi sekadar ancaman potensial, melainkan telah menjadi kenyataan. Tercatat antara tahun 2022 hingga 2023 terjadi peningkatan kasus penipuan berbasis *deepfake* hingga mencapai sekitar 1.550 persen.[2] Sebagai contoh, sektor keuangan mengalami kerugian yang sangat signifikan. Berdasarkan laporan yang diterbitkan oleh Indonesia Anti-Scam Center (IASC), sektor keuangan di Indonesia tercatat mengalami kerugian finansial yang signifikan, yaitu sekitar Rp700 miliar atau setara dengan 44 juta dolar Amerika Serikat dalam rentang waktu November 2024 hingga Februari 2025. Kerugian tersebut antara lain disebabkan oleh maraknya kasus penipuan yang memanfaatkan teknologi *deepfake*.[3]

Deepfake adalah teknologi yang memanfaatkan kecerdasan buatan *(AI)* untuk menghasilkan citra atau video sintetik yang tampak realistis dengan memanipulasi wajah atau suara individu.[4] Indonesia sebagai negara dengan penetrasi digital dan media sosial yang tinggi, menjadi salah satu negara yang rawan terhadap penyebaran konten *deepfake* yang merusak. Sayangnya, regulasi nasional belum memiliki perangkat hukum yang komprehensif dan adaptif dalam mengantisipasi penyalahgunaan teknologi berbasis *AI* ini. Indonesia, penggunaan teknologi *deepfake* secara ilegal semakin marak, terlebih dengan mudahnya masyarakat mengakses

[2] Uyu Septiyati Liman, "VIDA catat penipuan 'deepfake' di Indonesia melonjak 1.550 persen," *ANTARA NEWS*, 2024, https://www.antaranews.com/berita/4437365/vida-catat-penipuan-deepfake-di-indonesia-melonjak-1550-persen.

[3] Emanuel Edi Saputra, "Bank Digital Waspadai Penyalahgunaan Teknologi "Deepfake"," artikel, *kompas.id*, 2025, https://www.kompas.id/artikel/bank-digital-waspadai-penyalahgunaan-teknologi-deepfake?

[4] Meirza Aulia Chairani dkk., "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake," *JURNAL RECHTENS* 13, no. 1 (2024): 81–96, https://doi.org/10.56013/rechtens.v13i1.2668.

perangkat lunak pembuat *deepfake* melalui internet, namun kerangka hukum nasional masih belum memadai dalam mengantisipasi dan menanggulangi kejahatan berbasis *deepfake*.[5]

Penyalahgunaan teknologi *deepfake* di Indonesia menunjukkan dampak serius terhadap stabilitas sosial dan politik. Salah satu contohnya adalah video manipulatif Prabowo Subianto yang dibuat seolah-olah ia telah menjadi Presiden dan berjanji memberikan bantuan Rp50 juta kepada setiap warga.[6] Video ini menyesatkan publik dengan rekayasa visual dan audio yang tampak otentik, padahal sepenuhnya hasil manipulasi digital.[7] Kasus ini menimbulkan kerugian reputasi dan berpotensi menciptakan disinformasi politik berskala nasional, namun, pelaku hanya dapat dijerat dengan pasal umum dalam Undang-Undang ITE terkait penyebaran berita bohong, karena belum ada aturan spesifik yang mengatur kejahatan berbasis *AI deepfake*, menunjukkan adanya kekosongan hukum.

Kasus serupa terjadi pada April 2025, ketika tiga pelaku menipu publik melalui video *deepfake* yang meniru wajah dan suara tiga gubernur di Pulau Jawa Khofifah Indar Parawansa, Ahmad Luthfi, dan Dedi Mulyadi. Video tersebut memperlihatkan para gubernur seolah menawarkan sepeda motor murah untuk memancing masyarakat mentransfer uang ke rekening

[5] Chairani dkk., "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake," 2024.
[6] Alfitria Nefi Pratiwi, "Korban Penipuan Video Deepfake Prabowo Capai 100 Orang," *Tempo.co*, 2025, https://www.tempo.co/hukum/korban-penipuan-video-deepfake-prabowo-capai-100-orang-1204264.
[7] Yoan Shevila Kristiyenda dkk., "Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang," *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora* 3, no. 2 (2025): 149–64, https://doi.org/10.59246/aladalah.v3i2.1263.

pelaku.[8] Aksi ini menimbulkan kerugian finansial dan merusak kepercayaan publik terhadap pejabat pemerintah.

Kasus ini menunjukkan bahwa meskipun pelaku penyalahgunaan teknologi *deepfake* telah dijerat menggunakan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP), hingga saat ini belum terdapat regulasi khusus yang secara komprehensif mengatur tindak penyalahgunaan teknologi tersebut.[9] Kondisi ini menegaskan urgensi bagi Indonesia untuk meratifikasi Konvensi Budapest sebagai instrumen hukum internasional yang mengatur kejahatan siber, guna memperkuat sistem hukum nasional dalam menghadapi perkembangan teknologi informasi yang semakin rumit.[10]

Salah satu kasus yang gempar pada masanya ialah kasus *deepfake* Menteri Keuangan Sri Mulyani Indrawati menyebut guru sebagai beban negara. Kepala Biro Komunikasi dan Layanan Informasi Kementerian Keuangan Republik Indonesia, Deni Surjantoro, menegaskan bahwa potongan video yang beredar tersebut merupakan hoaks. Ia menjelaskan bahwa Menteri Keuangan tidak pernah menyampaikan pernyataan bahwa guru merupakan beban negara. Video yang tersebar itu

[8] Diva Rabiah, "Polda Jatim Ungkap Penipuan Deepfake 3 Gubernur Jualan Motor," Nasional, *metro tv news*, 30 April 2025, https://www.metrotvnews.com/play/kWDCnnVz-polda-jatim-ungkap-penipuan-deepfake-3-gubernur-jualan-motor.
[9] Desty Aster Yansen Basah dkk., "Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake di Media Sosial," *Innovative: Journal Of Social Science Research* Vol 5, no. 4 (2025): hal 8-9, https://doi.org/10.31004/innovative.v5i4.20258.
[10] Ida Ayu Agung Rasmi Wulan dan Ni Luh Gede Astariyani, "Urgensi dalam Meratifikasi Convention On Cybercrime sebagai Pemenuhan HAM di Indonesia," *Jurnal Kertha Patrika* vol 45 (Agustus 2023), https://doi.org/10.24843/KP.2023.v45.i02.p06.

merupakan hasil manipulasi teknologi *deepfake* serta penggalan yang tidak utuh dari pidato Sri Mulyani Indrawati dalam Forum Konvensi Sains, Teknologi, dan Industri Indonesia yang diselenggarakan di Institut Teknologi Bandung pada 7 Agustus.[11]

Dampak dari kasus tersebut, rumah pribadi Sri Mulyani beserta keluarganya dijarah hingga seluruh isinya hampir tidak tersisa oleh sekelompok orang yang tersulut emosi akibat pernyataan dalam video palsu tersebut. Peristiwa ini memperlihatkan betapa berbahayanya penyalahgunaan teknologi *deepfake*. Informasi yang direkayasa dapat membuat publik sulit membedakan mana yang benar dan mana yang tidak, sekaligus mencemarkan nama baik seseorang dan merusak kepercayaan terhadap informasi yang beredar di ruang publik.[12]

Konvensi Budapest secara resmi dibuka untuk penandatanganan pada tanggal 23 November 2001 di Budapest, Hungaria, setelah sebelumnya diadopsi oleh *Council of Europe* pada 8 November 2001. Instrumen hukum ini mulai berlaku efektif pada 1 Juli 2004, setelah terpenuhinya ketentuan mengenai jumlah minimum ratifikasi oleh negara-negara anggotanya.[13] Tujuan utama dari konvensi tersebut adalah untuk mewujudkan harmonisasi peraturan nasional yang berkaitan dengan tindak pidana siber, seperti akses

[11] Komdigi, "[Hoaks] Sri Mulyani Sebut Guru sebagai Beban Negara," *TBNews*, 2025, https://tribratanews.polri.go.id/blog/none-22/hoaks-sri-mulyani-sebut-guru-sebagai-beban-negara-92196.
[12] Ezra Pranata Tarigan dan I Nyoman Prabu Buana Rumiartha, "Kekosongan Hukum AI Di Indonesia: Kasus Deepfake Terhadap Sri Mulyani Dan Perbandingan Eu Ai Act," *Jurnal Media Akademik* vol 3, no. 11 (2025): 4, https://doi.org/10.62281/6vdqep64.
[13] Publications Office, "Convention on cybercrime," Access to European Union law, *EUR-Lex*, 2023, https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html?utm_source=chatgpt.com#.

tanpa izin, gangguan terhadap sistem elektronik, serta penyalahgunaan data digital dan konvensi ini juga bertujuan memperkuat mekanisme kerja sama internasional dalam pengumpulan dan pertukaran bukti elektronik serta penanganan perkara lintas yurisdiksi.[14]

Konvensi Budapest yang diinisiasi oleh *Council of Europe* memiliki cakupan yang bersifat global dan tidak terbatas pada kawasan Eropa. Berdasarkan Pasal 37, negara-negara di luar keanggotaan Dewan Eropa dapat berpartisipasi melalui undangan yang disetujui oleh mayoritas pihak anggota.[15] Peluang ini bisa menjadi kesempatan bagi Indonesia untuk menjadi bagian anggota dari Konvensi Budapest untuk menguatkan sistem hukum Indonesia.

Italia adalah negara pertama yang mengadopsi undang-undang tentang perlindungan AI khususnya *deepfake* dengan membuat Undang-Undang Nomor 132 Tahun 2025, yang mulai berlaku pada 10 Oktober 2025. Berkaitan dengan *deepfake*, undang-undang ini menghukum penyebaran konten yang dihasilkan atau diubah menggunakan kecerdasan buatan secara ilegal dengan hukuman penjara antara satu hingga lima tahun.[16] Italia telah memperkuat kerangka hukum, baik di ranah nasional maupun internasional.

Keterbatasan regulasi Indonesia dalam menghadapi dinamika kejahatan siber, khususnya dalam mencegah penyalahgunaan *deepfake*,

[14] "Convention on cybercrime."
[15] Strasbourg, "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols," *Council of Europe*, 2025, https://www.coe.int/en/web/cybercrime/the-budapest-convention?
[16] Simona Lavagnini, "Italy Adopted the First National Law on Artificial Intelligence," *AIPPI*, 2025, https://www.aippi.org/news/italy-adopted-the-first-national-law-on-artificial-intelligence/.

menimbulkan tantangan serius bagi Indonesia dalam menegakkan hukum terhadap pelaku yang beroperasi lintas batas negara.[17] Banyak di antara pelaku memanfaatkan server asing serta menyamarkan identitasnya, sehingga proses penegakan hukum menjadi tidak efektif. Jadi, urgensi ratifikasi Konvensi Budapest tentang Kejahatan Siber menjadi semakin relevan sebagai langkah strategis untuk memperkuat sistem hukum nasional melalui harmonisasi dengan standar hukum internasional.[18]

Kerangka hukum nasional, khususnya yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), hanya mengatur mengenai penyebaran informasi elektronik yang bermuatan penghinaan, pencemaran nama baik, atau konten yang melanggar kesusilaan, tanpa adanya ketentuan khusus mengenai manipulasi konten berbasis kecerdasan buatan yang dapat digunakan untuk menyesatkan publik atau menciptakan bukti palsu dalam suatu tindak pidana,[19] hal ini menunjukkan keterbatasan dalam menjamin efektivitas peran negara dalam menegakkan kedaulatan hukum di ruang siber. Kondisi tersebut tampak terutama ketika menghadapi bentuk kejahatan *deepfake* lintas yurisdiksi yang melibatkan penggunaan server luar negeri serta penyamaran identitas pelaku melalui anonimitas digital.

---

[17] Loso Judijanto dkk., "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia," *The Easta Journal Law and Human Rights* 3, no. 02 (2025): 105–7, https://doi.org/10.58812/eslhr.v3i02.470.

[18] Ayu Agung Rasmi Wulan dan Gede Astariyani, "Urgensi dalam Meratifikasi Convention On Cybercrime sebagai Pemenuhan HAM di Indonesia."

[19] Rafi Satrya Arvitto, "Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP," *Jurnal Ilmiah Hukum dan Hak Asasi Manusia* 4, no. 2 (2025): 73–82, https://doi.org/10.35912/jihham.v4i2.3937.

Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan sebagai upaya memperkuat keamanan informasi di ruang digital juga belum sepenuhnya memberikan perlindungan komprehensif terhadap penyalahgunaan teknologi berbasis kecerdasan buatan seperti *deepfake*.[20] Pengaturan dalam Undang-Undang tersebut masih berfokus pada aspek perlindungan data individu,[21] sementara dimensi kejahatan siber yang bersifat lintas batas dan melibatkan manipulasi digital memerlukan mekanisme kerja sama internasional yang lebih terintegrasi dan efektif.

Menteri Komunikasi dan Informatika juga telah menerbitkan Surat Edaran Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. Surat Edaran tersebut dapat dipandang sebagai upaya awal yang cukup progresif dalam menanamkan prinsip-prinsip etika pada pengembangan dan pemanfaatan kecerdasan buatan di Indonesia. Surat Edaran tersebut menekankan sejumlah nilai fundamental, seperti inklusivitas, kemanusiaan, keamanan, transparansi, kredibilitas dan akuntabilitas, pelindungan data pribadi, pembangunan dan lingkungan berkelanjutan serta kekayaan lntelektual.[22] Prinsip-prinsip yang diatur di dalamnya menjadi relevan ketika dikaitkan dengan persoalan *deepfake*, mengingat teknologi ini kerap

[20] Rafi Satrya Arvitto, Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP *(Legal Implications of Deepfake: A Review of the ITE Law and the PDP Law)*, 4, no. 2 (2025).
[21] Muhammad Ariq Abir Jufri dan Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 31–57, https://doi.org/10.22437/up.v2i1.11093.
[22] Abul Muamar, "Kominfo Terbitkan Surat Edaran terkait Etika Penggunaan AI," *green network*, 2024, https://greennetwork.id/gna-knowledge-hub/kominfo-terbitkan-surat-edaran-terkait-etika-penggunaan-ai/.

digunakan dengan cara yang melanggar hak privasi, merusak reputasi serta kredibilitas seseorang.

Kelemahan dari Surat Edaran ini ialah tidak memiliki kekuatan mengikat secara hukum dan lebih berfungsi sebagai imbauan serta pedoman, efektivitasnya sebagai alat penegakan hukum menjadi terbatas.[23] Surat Edaran tersebut juga belum mengatur secara tegas mekanisme pemberian sanksi, tata cara investigasi khusus terhadap kejahatan siber berbasis kecerdasan buatan khususnya *AI deepfake*, maupun kerangka kerja sama internasional yang memadai untuk menindak pelaku yang kerap beroperasi lintas yurisdiksi negara. Kondisi ini memperlihatkan adanya kekosongan pengaturan yang menegaskan perlunya peraturan hukum yang lebih kuat, menyeluruh, dan memiliki daya ikat yang jelas.

Teori *State Responsibility and Due Diligence* dari James Crawford menekankan bahwa negara dapat dimintai pertanggungjawaban bukan hanya atas tindakannya, tetapi juga kelalaiannya dalam mencegah pelanggaran hukum internasional. Prinsip ini mengharuskan negara menjalankan *due diligence* dengan memastikan wilayahnya tidak digunakan untuk aktivitas yang merugikan pihak lain maupun melanggar hak-hak individu.[24] Teori ini dalam konteks penyalahgunaan *deepfake* di Indoensia sangat relevan, letak relevansinya pada kewajiban negara untuk tidak hanya

[23] Misrohatun H, "Kominfo Terbitkan Surat Edaran Etika Penggunaan dan Pemanfaatan AI," *IDN TIMES*, 2023, https://www.idntimes.com/tech/trend/kominfo-terbitkan-surat-edaran-etika-penggunaan-dan-pemanfaatan-ai-00-h7csw-dpvng4.
[24] Nadezhda N. Lipkina dan Dmitry V. Krasikov, "The International Legal Obligation Of Due Diligence In Cyberspace," 20 Januari 2022, 392–97, https://doi.org/10.15405/epsbs.2022.01.63.

bertindak aktif dalam mencegah pelanggaran hukum internasional, tetapi juga menghindari kelalaian yang memungkinkan tindak kejahatan lintas batas, termasuk penyalahgunaan *deepfake*.[25] Indonesia yang hingga kini belum meratifikasi Konvensi Budapest menunjukkan adanya kesenjangan antara tanggung jawab normatif negara dalam hukum internasional dan ketersediaan instrumen hukum di tingkat nasional.

Tanpa ratifikasi, Indonesia berpotensi dianggap lalai karena belum memiliki kerangka kerja sama internasional yang memadai untuk menindak dan mencegah *deepfake* yang berdampak lintas negara.Tanpa regulasi dan kerja sama internasional yang memadai, kelalaian negara dapat dipandang sebagai kegagalan memenuhi kewajiban hukum internasional. Apabila Indonesia telah meratifikasi Konvensi Budapest, kedudukan hukumnya akan semakin kokoh, baik dalam lingkup nasional maupun internasional.[26]

Perspektif *maqāṣid ash-sharīʿah* memandang penyalahgunaan teknologi deepfake bukan semata-mata sebagai permasalahan teknis atau kekosongan regulasi, melainkan juga sebagai isu yang berkaitan dengan tujuan syariah dalam menjaga kemaslahatan dan mencegah kemudaratan (mafsadah).[27] Pendekatan maqāṣid ash-Sharīʿah menurut Imam Ghazali

[25] Joni Laksito dkk., "Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif," *Hakim: Jurnal Ilmu Hukum dan Sosial* 2, no. 4 (2024): 774–90, https://doi.org/10.51903/hakim.v2i4.2154.
[26] Saptha Nugraha Isa dkk., "Criminal Law Policy in Dealing With The Development of Transnational Cyber Crime," *International Journal of Sociology and Law* Vol 2, no. 2 (2025): 118, https://doi.org/10.62951/ijsl.v2i2.652.
[27] Zainal Abidin, "Urgensi Maqashid Syariah bagi Kemashlahatan Umat," *Jurnal Kajian Keislaman* vol 1 (2023): hlm 126.

menekankan tujuan-tujuan utama syariah untuk menjaga lima hal pokok: agama *(dīn)*, jiwa (*nafs*), akal *(ʿaql),* keturunan (nasl) dan harta (*māl*).[28]

Hifẓ al-ʿaql (menjaga akal) dan *ḥifẓ an-nafs* (menjaga jiwa), penyebaran konten *deepfake* tanpa kendali dapat mengganggu nalar sehat masyarakat, memicu fitnah, serta menimbulkan tekanan psikologis bagi individu yang menjadi korban. Aspek *ḥifẓ al-māl* (menjaga harta) dan *ḥifẓ an-nasl* (menjaga keturunan) juga berpotensi terganggu, mengingat reputasi, kehormatan keluarga, serta stabilitas ekonomi dapat dirusak melalui penyebaran konten manipulatif. Selain itu, nilai *ḥifẓ ad-dīn* (menjaga agama) dan kemaslahatan sosial dapat terdegradasi apabila teknologi manipulasi digital digunakan untuk menyebarkan disinformasi yang merusak kepercayaan publik dan menimbulkan disintegrasi moral.[29]

B. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana urgensi ratifikasi Konvensi Budapest dalam upaya pencegahan penyalahgunaan *deepfake* di Indonesia berdasarkan teori Tanggung Jawab Negara (*State Responsibility*)?
2. Bagaimana pengaturan *deepfake* di Indonesia dan Italia ?
3. Bagaimana urgensi pengaturan pencegahan penyalahgunaan *deepfake* di Indonesia perspektif *Maqashid Syariah* ?

[28] Tim Hukum Online, "Mengenal Tujuan dan Tingkatan 5 Maqashid Syariah," *Hukumonline.com*, 2024, https://www.hukumonline.com/berita/a/maqashid-syariah-lt65c063a25e4c6/.
[29] Ahmer Bilal Soofi dan Muhammad Khalid Masud, *International Law and Maqasid Al-Shariah*, 2024, hal 2-3.

C. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan dari penelitian ini adalah sebagai berikut :

1. Menganalisis dan mengkaji urgensi ratifikasi Konvensi Budapest berdasarkan teori tanggung jawab negara.
2. Menganalisis dan mendeskripsikan pengaturan *deepfake* di Indonesia dan Italia.
3. Mennganalisis dan mendeskripsikan urgensi pengaturan pencegahan penyalahgunaan *deepfake* di Indonesia perspektif *Maqashid Syariah*.

D. Manfaat Penelitian

1. Manfaat Teoritis

   Penelitian ini dapat memberikan kontribusi pemikiran tentang pentingnya ratifikasi Konvensi Budapest sebagai dasar penguatan sistem hukum nasional dalam mencegah penyalahgunaan *deepfake* di Indonesia.

2. Manfaat Praktisi

   Penelitian ini dapat menjadi masukkan bagi pemerintah Indonesia dalam mempertimbangkan ratifikasi Konvensi Budapest, guna memperkuat mekanisme hukum dalam mencegah penyalahgunaan *deepfake* di Indonesia.

E. Definisi Konseptual

Definisi konseptual merupakan penjelasan terhadap konsep yang ada dalam judul penelitian. Tujuan dari adanya penjelasan ini guna memahami

dan membatasi dengan jelas penafsiran peneliti agar tidak menimbulkan multitafsir. Beberapa istilah yang dirasa perlu diberi penjelasan berdasarkan judul "Urgensi Pengaturan Penyalahgunaan *Deepfake* Di Indonesia Perspektif Teori Tanggung Jawab Negara Dan *Maqashid Syariah*"

1. Urgensi

   Urgensi adalah keharusan yang mendesak atau hal yang sangat penting yang memerlukan perhatian dan tindakan segera. Istilah ini berasal dari kata bahasa Inggris *"urgent"* yang berarti kepentingan mendesak, dan dalam Kamus Besar Bahasa Indonesia (KBBI) diartikan sebagai sesuatu yang harus segera diselesaikan karena sifatnya yang penting dan mendesak.[30]

   Menurut kamus Cambridge: *"the quality of being very important and needing attention immediately"* yang artiannya bahwa urgensi ialah mengacu pada kondisi atau kualitas sesuatu yang sangat penting dan memerlukan perhatian atau tindakan segera.[31]

2. Pengaturan

   Pengaturan dapat dipahami sebagai rangkaian proses atau tindakan untuk mengatur sesuatu melalui penetapan tatanan, pedoman, kaidah, maupun ketentuan tertentu.[32] Pengaturan ini bertujuan untuk

[30] Luqman Hakim, "Urgensi Adalah: Pengertian, Jenis, dan Cara Menghadapi," *deepublish*, 2024, https://deepublishstore.com/blog/urgensi/.
[31] Liz Walter, "Cambridge Dictionary," dalam *Cambridge Dictionary* (Cambridge University Press & Assessment, 2025), Cambridge Dictionary.
[32] Mykhailo Kelman dan Rostislav Kelman, "Doctrine approaches to the disclousure of the concept of 'Legal regulation,'" *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki* 10, no. 39 (2023): 13, https://doi.org/10.23939/law2023.39.013.

mengendalikan dan menata suatu objek atau aktivitas agar pelaksanaannya berlangsung secara tertib, terarah, dan sesuai dengan tujuan yang telah ditetapkan.

Menurut KBBI pengaturan adalah cara (perbuatan) mengatur. Menurut *Encyclopaedia Britannica* pengaturan adalah merujuk pada aturan-aturan yang mengatur perilaku individu dalam konteks tertentu tanpa mendalilkan dari mana aturan-aturan tersebut berasal dan bagaimana aturan-aturan tersebut diterapkan.[33]

3. *Deepfake*

Deepfake merujuk pada bentuk media berupa gambar, video, atau audio yang dibuat maupun dimodifikasi dengan memanfaatkan teknologi kecerdasan buatan *(artificial intelligence)* sehingga menampilkan seseorang seolah-olah melakukan atau mengucapkan sesuatu yang sebenarnya tidak pernah dilakukan ataupun diucapkan.[34] Teknologi ini bekerja dengan menggabungkan konsep *deep learning* dan unsur pemalsuan *(fake),* yang kemudian membentuk istilah *deepfake* untuk menggambarkan hasil manipulasi digital berteknologi tinggi tersebut.[35]

---

[33] Cornelia Woll, "Regulation," dalam *Britannica*, 2025, https://www.britannica.com/topic/regulation.
[34] Itsna Hidayatul Khusna Sri Pangestuti, "Deepfake, Tantangan Baru Untuk Netizen," *PROMEDIA* Vol 5 (2020): 6.
[35] Kinza Yasar, "What is deepfake technology?," *TechTarget*, 2025, https://www.techtarget.com/whatis/definition/deepfake?

4. Tanggung Jawab Negara (*State responsibility*)

Tanggung jawab negara merupakan salah satu prinsip inti dalam hukum internasional yang berkembang dari sifat dasar sistem hukum internasional itu sendiri, serta bertumpu pada doktrin kedaulatan dan kesetaraan negara. Prinsip ini menunjukkan bahwa setiap tindakan negara yang melanggar hukum internasional dan merugikan negara lain akan menimbulkan konsekuensi berupa tanggung jawab internasional. Konteks tersebut, pelanggaran terhadap kewajiban internasional mewajibkan negara pelaku untuk memberikan ganti rugi atas kerugian yang ditimbulkan.[36]

5. *Maqashid Syariah*

Maqashid al-syariah menurut Imam Ghazali adalah bahwa *maqashid syariah* adalah upaya syariat untuk mewujudkan kemaslahatan dan menolak kerusakan. Imam al-Ghazali memaknai maqashid melalui konsep maslahah yang bersifat menjaga kebutuhan dasar manusia.[37]

Imam al-Ghazali membangun struktur maqashid pada lima perlindungan pokok yang dikenal sebagai *al-dharuriyat al-khams,* yaitu *ḥifẓ al-dīn* (agama), *ḥifẓ al-nafs* (jiwa), *ḥifẓ al-'aql* (akal), *ḥifẓ al-nasl* (keturunan), dan *ḥifẓ al-māl* (harta)

[36] Nurilloev Shavkat Shukhrat Ugli, "The Foundations Of State Responsibility In International Law: An In-Depth Analysis Of Key Principles And Norms," *European Journal of Contemporary Business Law & Technology: Cyber Law, Blockchain, and Legal Innovations* 1, no. 9 (2024): 100, https://doi.org/10.61796/ejcblt.v1i9.1031.

[37] Noor Harisudin, *Maqashid Syariah: Metode Subtantif Menuju Hukum Keluarga Baru*, cetakan pertama (CV. Literasi Nusantara Abadi, 2022), 24.

Secara substansial dalam menetapkan suatu hukum perlu terlebih dahulu dipahami tujuan dari hukum atau syariah itu sendiri, yaitu untuk mewujudkan kemaslahatan bagi manusia, baik di kehidupan dunia maupun di akhirat.[38]

F. Metode Penelitian

1. Jenis Penelitian

   Jenis penelitian yang digunakan oleh penulis adalah penelitian yuridis normatif yaitu pendekatan dalam penelitian hukum yang dilakukan berdasarkan bahan hukum utama, seperti teori-teori, konsep-konsep, dan asas-asas hukum.[39] Pendekatan ini menelaah hukum sebagai apa yang tertulis dalam peraturan perundang-undangan atau sebagai kaidah atau norma yang menjadi patokan perilaku manusia yang dianggap pantas.

   Metode penelitian ini menggunakan bahan pustaka atau bahan sekunder, dan merupakan penelitian terhadap sistematis hukum untuk mengidentifikasi pengertian, asas, norma, kaidah dari peraturan perundangan, perjanjian, serta doktrin. Pendekatan yuridis normatif dikenal juga dengan pendekatan kepustakaan, di mana peneliti

[38] Paryadi, "Maqashid Syariah : Definisi Dan Pendapat Para Ulama," *Universitas Islam Negeri Sultan Syarif Kasim Riau* Vol 4, no. 2 (2021): 215.
[39] Kornelius Benuf dan Muhamad Azhar, "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Jurnal Gema Keadilan* Vol 7, no. 1 (2020): 23–24.

mempelajari buku, peraturan perundang-undangan, dan dokumen lain yang terkait dengan penelitiannya.[40]

2. Pendekatan Penelitian

Metode pendekatan penelitian ini adalah penelitian ini menggunakan metode pendekatan Undang – Undang (*Statue Approach*) yaitu pendekatan penelitian yang dilakukan dengan menelaah semua Undang – Undang dan regulasi yang berkaitan dengan isu dan permasalahan – permasalahan hukum yang sedang ditangani.[41] Pendekatan yang dilakukan dalam penelitian ini ialah pendekatan perundang – undangan yang akan diteliti adalah Konvensi/Perjanjian Budapest tentang Kejahatan Siber *(Budapest Convention on Cybercrime).*

Isu hukum yang digunakan dalam penelitian ini adalah *legal vacuum* atau kekosongan hukum dalam pengaturan penyalahgunaan teknologi *deepfake* di Indonesia. Kekosongan hukum adalah kondisi ketika suatu perbuatan atau fenomena yang memiliki dampak hukum tidak atau belum secara jelas diatur dalam sistem perundang-undangan yang berlaku.[42] Penelitian ini juga menggunakan pendekatan konseptual *(conceptual approach),* yakni pendekatan yang bertitik tolak dari konsep-konsep hukum yang relevan, baik yang berkembang dalam teori maupun yang tertuang dalam instrumen hukum internasional dan

[40] Wiwik Sri Widiarty, *Metode Penelitian Hukum*, cetakan pertama (Publika Global Media, 2024), 19.
[41] Muhaimin, *Metode Penelitian Hukum*, cetakan pertama (Mataram University Press, 2020), 56.
[42] Abdullah Sulaiman, *Pengantar Ilmu Hukum*, cetakan kedua (UIN Jakarta bersama Yayasan Pendidikan dan Pengembangan Sumber Daya Manusia, 2020).

nasional.[43] Pendekatan ini digunakan untuk menganalisis secara mendalam konsep ratifikasi perjanjian internasional, kejahatan siber berbasis *deepfake*, serta nilai-nilai *maqashid syariah*.

Penelitian ini juga menggunakan pendekatan komparatif (*comparative approach*) yaitu pendekatan yang menelaah dan membandingkan sistem hukum atau peraturan perundang-undangan suatu negara dengan peraturan di satu atau beberapa negara lain yang mengatur isu serupa. Melalui perbandingan tersebut, dapat diketahui berbagai persamaan maupun perbedaan di antara masing-masing sistem hukum tersebut.[44] Negara yang akan dibandingkan ialah Italia dengan Indonesia.

3. Bahan Hukum

   Penelitian hukum normatif menggunakan teknik pengumpulan data melalui studi pustaka terhadap berbagai sumber hukum, yang mencakup bahan hukum primer, sekunder, dan tersier.

   a. Bahan Hukum Primer

      Bahan hukum primer adalah sumber hukum yang mempunyai kekuatan mengikat secara sah. Bentuknya dapat berupa peraturan perundang-undangan seperti undang-undang, peraturan pemerintah, hingga peraturan daerah. Bahan hukum primer juga mencakup regulasi resmi pembentukan undang-undang, putusan pengadilan yang telah menjadi yurisprudensi, serta perjanjian atau traktat

[43] *Metode Penelitian Hukum*, 57.
[44] *Metode Penelitian Hukum*, 57.

internasional.[45] Dalam penelitian ini bahan hukum primer yang digunakan meliputi:

1) *Konvensi Budapest on Cybercrime* (2001), Pasal 2-9
2) Undang-Undang Italia Nomor 132 Tahun 2025 tentang Ketentuan dan Kewenangan kepada Pemerintah terkait Kecerdasan Buatan, Pasal 612-quater dan Pasal 4 ayat (2)
3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28F, Pasal 28G ayat (1) dan Pasal 28I ayat (4)
4) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 4 dan Pasal 65-67
5) Undang-Undang Nomor 1 Tahun 2024 perubahan atas Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Pasal 27 ayat (1), Pasal 27A, Pasal 28 ayat (1), Pasal 28 ayat (2), Pasal 28 ayat (3), Pasal 29, Pasal 36, Pasal 45, 45A dan 45B
6) Undang-Undang Nomor 24 Tahun 2000 tentang Perjanjian Internasional, Pasal 9 dan 10
7) Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial

[45] Muhammad Citra Ramadhan, *Buku Ajar - Metode Penelitian Hukum* (CV. Kaizen Sarana Edukasi, 2023), 75.

b. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan yang tidak diperoleh peneliti secara langsung dari objek yang diteliti, melainkan melalui berbagai rujukan lain, baik tertulis maupun lisan. Contohnya meliputi buku, artikel ilmiah, jurnal, majalah, surat kabar, dokumen.[46]

Bahan hukum sekunder yang menjadi penunjang bahan hukum primer dalam penelitian ini adalah hasil penelitian terdahulu, Jurnal Ilmiah, Opini dan Berita.

c. Bahan Hukum Tersier

Bahan hukum tersier adalah jenis rujukan yang membantu menjelaskan dan memperjelas isi bahan hukum primer maupun sekunder. Bentuknya bisa berupa kamus, ensiklopedia, leksikon, atau sumber penjelas lainnya.[47]

Bahan hukum tersier yang digunakan penulis dalam penelitian ini, selain bahan hukum primer dan sekunder, meliputi kamus hukum, ensiklopedia, serta sumber-sumber pendukung lainnya.

1) Kamus Besar Bahasa Indonesia (KBBI)
2) Kamus Hukum (Dictionary Of Law)
3) Cambridge Dictionary
4) Oxford Dictionary

[46] Nur Solikin, *Pengantar Metodologi Penelitian Hukum*, cetakan pertama (CV. Penerbit Qiara Media, 2021).
[47] Sigit Sapto Nugroho dkk., *Metodologi Riset Hukum*, cetakan pertama (Oase Pustaka, 2020), 68.

4. Teknik Pengumpulan Bahan Hukum

   Teknik pengumpulan bahan hukum yang digunakan penulis dilakukan melalui studi kepustakaan *(library research)* serta penelusuran melalui akses internet. Kegiatan ini dilakukan dengan menelaah berbagai literatur, peraturan perundang-undangan, artikel, karya ilmiah, serta sumber dari media cetak dan elektronik yang relevan dengan topik penelitian.[48] Studi kepustakaan *(library research)* sendiri merupakan kegiatan mengkaji berbagai informasi tertulis mengenai hukum yang bersumber dari berbagai publikasi dan digunakan sebagai dasar dalam penelitian hukum normatif.[49]

5. Metode Pengolahan Bahan Hukum

   Karakteristik analisis dalam penelitian hukum normatif ini bersifat deskriptif-analitis. Menurut Sugiono, metode deskriptif merupakan metode penelitian yang bertujuan untuk menggambarkan atau menjelaskan objek yang diteliti berdasarkan data atau sampel yang telah diperoleh sebagaimana adanya, tanpa melakukan analisis lebih lanjut maupun menarik kesimpulan yang bersifat umum.[50]

[48] Ahamad Rosidi dkk., "Metode Dalam Penelitian Hukum Normatif Dan Sosiologis (Field Research)," *Journal Law and Government* 2, no. 1 (2024): 52, https://doi.org/10.31764/jlag.v2i1.21606.
[49] Eko Haryono dkk., "New Paradigm Metode Penelitian Kepustakaan (Library Research) di Perguruan Tinggi," *An-Nur: The Journal of Islamic Studies* Vol 14, no. 1 (2024): 3.
[50] Siti Faridah, "Adapun Pengertian Dari Metode Deskriptif Analitis Menurut Sugiono," scribd, 2016, https://www.scribd.com/doc/306349047/Adapun-Pengertian-Dari-Metode-Deskriptif-Analitis-Menurut-Sugiono.

Oleh karena itu, pengolahan bahan hukum dilakukan dengan metode interpretasi normatif melalui pendekatan gramatikal, sistematis, dan teleologis.

G. Penelitian Terdahulu

Penelitian mengenai penyalahgunaan teknologi digital, khususnya terkait kejahatan siber seperti penggunaan *deepfake*, telah dilakukan oleh beberapa peneliti sebelumnya, meskipun dengan fokus dan sudut pandang yang berbeda-beda. Untuk melengkapi data dalam penelitian ini serta menghindari terjadinya duplikasi pembahasan, diperlukan telaah terhadap penelitian terdahulu yang memiliki keterkaitan substansial. Adapun beberapa penelitian sebelumnya yang membahas isu kejahatan siber, regulasi digital, dan urgensi kerja sama internasional dalam konteks hukum siber dapat dijadikan sebagai landasan komparatif dalam penelitian ini :

1. Jurnal oleh Jeremiah Maximillian Laza dan Rizky Karo Karo yang terbit di Jurnal Lex Prospicit pada 2 Juli 2023 dengan judul "Perlindungan Hukum Terhadap Kecerdasan Buatan Dalam Aspek Penyalahgunaan Teknologi Deepfake Pada Perspektif UU PDP dan GDPR [Perlindungan Hukum atas Kecerdasan Buatan dalam Penyalahgunaan Teknologi *Deepfake* dalam Perspektif UU PDP dan GDPR]". Penelitian ini menggunakan metode penelitian hukum normatif menggunakan bahan hukum primer, sekunder, dan tersier. Penelitian ini bertujuan untuk mengkaji perlindungan hukum terhadap teknologi *deepfake* berbasis *AI*

dari perspektif regulasi yang ada, yaitu GDPR di Eropa dan UU PDP di Indonesia. Hasil penelitian tersebut menunjukkan bahwa :[51]

Penggunaan pengaturan *deepfake* dalam *General Data Protection Regulation* (GDPR) dan bagaimana UU PDP Indonesia meminta pertanggungjawaban hukum dari pelaku *deepfake* sebagai tindak pidana penipuan atau membuat berita bohong. Pengaturan hukum saat ini, baik dari GDPR di Eropa maupun UU PDP di Indonesia, secara tidak langsung sudah mencakup perlindungan terhadap aspek-aspek yang berkaitan dengan *deepfake*, terutama yang terkait penggunaan data pribadi dan manipulasi informasi digital, namun kedua regulasi tersebut tidak secara khusus mengatur tentang *deepfake* sebagai fenomena *AI* yang merugikan, sehingga terdapat kekosongan regulasi yang spesifik dan mendalam mengenai penanggulangan serta pencegahan *deepfake* secara langsung. Oleh karena itu, diperlukan pengembangan regulasi yang lebih tajam dan spesifik untuk mengatur penggunaan *AI* dan *deepfake* agar dapat melindungi subjek hukum secara lebih efektif serta menyeimbangkan antara inovasi teknologi dan perlindungan hak asasi manusia.

Perbedaan penelitian tersebut dengan penelitian yang akan dilakukan oleh penulis terletak pada pembahasanya, jurnal ini berfokus

[51] Jeremiah Maximillian Laza dan Rizky Karo Karo, "Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP dan GDPR [Legal Protection of Artificial Intellegence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR]," *Lex Prospicit* 1, no. 2 (2023): 136, https://doi.org/10.19166/lp.v1i2.7386.

terhadap pada perlindungan hukum terhadap teknologi *deepfake* berbasis *AI*, dengan meninjau regulasi GDPR di Eropa dan UU PDP di Indonesia, sedangkan penelitian yang akan dilakukan oleh penulis fokus terhadap kebutuhan mendesak (urgensi) bagi Indonesia untuk meratifikasi Konvensi Budapest, yang merupakan instrumen hukum internasional tentang kejahatan siber, khususnya dalam konteks penyalahgunaan teknologi *deepfake*, dengan pendekatan perspektif *maqashid syariah*.

2. Jurnal oleh Muhammad Ariq Abir Jufri dan Akbar Kurnia yang terbit di Uti Possidetis: Journal of International Law pada 18 Maret 2021 dengan judul "Aspek Hukum Internasional Dalam Pemanfaatan Teknologi *Deepfake* Terhadap Perlindungan Data Pribadi". Penelitian ini menggunakan metode penelitian hukum normatif menggunakan bahan hukum primer, sekunder, dan tersier. Penelitian ini bertujuan untuk mengetahui aspek-aspek hukum internasional dalam pemanfaatan *Deepfake Technology* terhadap perlindungan data pribadi dan dampaknya terhadap hukum nasional Indonesia berdasarkan dengan Prinsip Hukum *Social Engineering* yaitu hukum diciptakan sebagai sedemikian rupa untuk mengarahkan perubahan ke arah yang lebih baik dan *Social Controlling* merupakan proses yang direncanakan untuk memaksa seseorang untuk mentaati kebiasaan, norma dan nilai hidup di masyarakat agar tidak terjadinya perilaku menyimpang dalam pemanfaatan teknologi *Deepfake* serta cara menyelaraskan aturan

hukum internasional dengan prinsip *Planning*, *Organizing*, *Actuating* dan *Controlling*. Hasil penelitian tersebut menunjukkan bahwa:[52]

Saat ini belum terdapat regulasi yang secara khusus mengatur penggunaan teknologi *Deepfake* secara langsung. Faktanya dibutuhkan langkah strategis untuk menyelaraskan hukum internasional dan nasional dalam hal perlindungan data pribadi dan penanggulangan penyalahgunaan *Deepfake*, dengan mengacu pada prinsip-prinsip perencanaan, pengorganisasian, pelaksanaan, dan pengawasan. Penelitian ini juga menyoroti pentingnya kolaborasi internasional, khususnya melalui lembaga seperti *International Telecommunication Union*, guna membentuk standar dan regulasi global yang mampu merespons tantangan hukum akibat pemanfaatan teknologi *Deepfake*, di sisi lain perlu juga disusun regulasi nasional yang sesuai dengan ketentuan hukum yang berlaku untuk secara efektif mengatasi penyalahgunaan teknologi tersebut.

Perbedaan penelitian tersebut dengan penelitian yang akan dilakukan oleh penulis terletak pada pembahasanya, jurnal ini berfokus terhadap pada aspek hukum internasional dan nasional terkait pemanfaatan teknologi *Deepfake*, terutama dalam konteks perlindungan data pribadi dan penyalahgunaannya, sedangkan penelitian yang akan dilakukan oleh penulis fokus terhadap kebutuhan mendesak (urgensi)

[52] Jufri dan Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi."

bagi Indonesia untuk meratifikasi Konvensi Budapest, yang merupakan instrumen hukum internasional tentang kejahatan siber, khususnya dalam konteks penyalahgunaan teknologi *deepfake*, dengan pendekatan perspektif *maqashid syariah*.

3. Jurnal oleh Ermanto Fahamsyah,Vicko Taniady,Kania Venisa Rachim, dan Novi Wahyu Riwayanti yang terbit di Jurnal De Jure: Jurnal Hukum dan Syariah pada 29 Juni 2022 dengan judul "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention". Penelitian ini menggunakan metode penelitian hukum normatif menggunakan bahan hukum primer, sekunder, dan tersier. Penelitian ini bertujuan untuk mengkaji problematika penanganan bagi pelaku cybercrime lintas negara serta mengkaji solusi penerapan prinsip Aut Dedere Aut Judicare melalui upaya ratifikasi Budapest Convention. Hasil penelitian tersebut menunjukkan bahwa:[53]

   Indonesia hingga saat ini belum memiliki pengaturan khusus yang mengatur *cybercrime*, meski pun sudah terdapat beberapa peraturan seperti KUHP dan UU ITE, namun kedua peraturan tersebut masih belum mampu menangani secara efektif para pelaku *cybercrime* lintas negara, terutama terkait permasalahan yurisdiksi. Jadi, penerapan prinsip *Aut Dedere Aut Judicare* melalui ratifikasi Budapest Convention

[53] Ermanto Fahamsyah dkk., "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention," *De Jure: Jurnal Hukum dan Syar'iah* 14, no. 1 (2022): 140–59, https://doi.org/10.18860/j-fsh.v14i1.15731.

sangat penting dan mendesak dilakukan sebagai dasar hukum untuk meningkatkan kerjasama internasional dalam penanganan *cybercrime* lintas negara.

Perbedaan penelitian tersebut dengan penelitian yang akan dilakukan oleh penulis terletak pada pembahasanya, jurnal ini berfokus terhadap mengenai problematika pengaturan pidana bagi pelaku *cybercrime* lintas negara di Indonesia serta solusi penerapan prinsip *Aut Dedere Aut Judicare* melalui upaya ratifikasi *Budapest Convention*, sedangkan penelitian yang akan dilakukan oleh penulis fokus terhadap kebutuhan mendesak (urgensi) bagi Indonesia untuk meratifikasi Konvensi Budapest, yang merupakan instrumen hukum internasional tentang kejahatan siber, khususnya dalam konteks penyalahgunaan teknologi *deepfake*, dengan pendekatan perspektif *maqashid syariah*.

4. Jurnal oleh Meirza Aulia Chairani,Krista Yitawati dan Angga Pramodya Pradhana yang terbit di Jurnal Rechtens pada 22 Juni 2024 dengan judul "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake". Penelitian ini menggunakan metode penelitian hukum normatif menggunakan bahan hukum primer, sekunder, dan tersier. Penelitian ini bertujuan untuk mengkaji bentuk atau tindakan penyalahgunaan aplikasi *Deepfake* yang dilakukan oleh pelaku tindak pidana serta untuk mengkaji ketentuan hukum pidana yang diterapkan

terhadap pelaku penyalahgunaan aplikasi *Deepfake* tersebut. Hasil penelitian tersebut menunjukkan bahwa:[54]

Penyalahgunaan aplikasi *Deepfake* telah berpotensi menimbulkan berbagai kejahatan seperti pornografi, pencurian data pribadi, dan penipuan melalui modifikasi wajah dan suara tanpa izin. Selain itu, pemerintah sampai saat ini belum memiliki peraturan hukum yang spesifik dan rinci mengenai penggunaan *Deepfake*, sehingga korban sulit memperoleh perlindungan hukum yang memadai, dan pelaku penyalahgunaan cenderung tidak mendapatkan efek jera karena kurangnya norma hukum yang mengatur secara tegas.

Perbedaan penelitian tersebut dengan penelitian yang akan dilakukan oleh penulis terletak pada pembahasanya, jurnal ini berfokus terhadap mengenai bentuk atau tindakan penyalahgunaan aplikasi *Deepfake* yang dilakukan oleh pelaku tindak pidana serta analisis tentang ketentuan hukum pidana yang diterapkan terhadap pelaku tersebut serta membahas isu-isu terkait perkembangan teknologi *AI*, dampaknya terhadap masyarakat, dan pentingnya pengaturan hukum yang efektif untuk mengatasi penyalahgunaan *Deepfake* guna melindungi korban dan menertibkan penggunaan teknologi ini secara hukum, sedangkan penelitian yang akan dilakukan oleh penulis fokus terhadap kebutuhan mendesak (urgensi) bagi Indonesia untuk

[54] Meirza Aulia Chairani dkk., "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake," *Jurnal Rechtens* 13, no. 1 (2024): 81–96, https://doi.org/10.56013/rechtens.v13i1.2668.

meratifikasi Konvensi Budapest, yang merupakan instrumen hukum internasional tentang kejahatan siber, khususnya dalam konteks penyalahgunaan teknologi *deepfake*, dengan pendekatan perspektif *maqashid syariah*.

5. Jurnal oleh Chiquita Thefirstly Noerman dan Aji Lukman Ibrahim yang terbit di Jurnal USM Law Review pada 3 Juni 2024 dengan judul "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindung Negara". Penelitian ini menggunakan metode penelitian hukum normatif yang menggunakan 3 (tiga) pendekatan, yaitu pendekatan perundang-undangan, pendekatan perbandingan, dan pendekatan konseptual. Penelitian ini bertujuan untuk mengetahui regulasi terkait kejahatan *deepfake* di Indonesia dan mengetahui regulasi ideal terkait kejahatan *deepfake* di masa mendatang. Hasil penelitian tersebut menunjukkan bahwa:[55]

   Indonesia belum secara tegas mengatur kejahatan *deepfake*. Indonesia hanya mengatur pemalsuan data pribadi secara umum dalam UU PDP dan juga pemalsuan elektronik dalam UU ITE yang merupakan turunan UUD NRI 1945. Penyalahgunaan aplikasi *Deepfake* telah menyebabkan berbagai kejahatan seperti pornografi, pencurian data pribadi, penipuan, dan kerusakan reputasi. Selain itu, masih terdapat kekurangan regulasi hukum yang khusus dan rinci mengenai

[55] Chiquita Thefirstly Noerman dan Aji Lukman Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara," *Jurnal Usm Law Review* 7, no. 2 (2024): 603–21, https://doi.org/10.26623/julr.v7i2.8995.

penggunaan *Deepfake* di Indonesia, sehingga korban sulit memperoleh perlindungan hukum yang memadai dan pelaku penyalahgunaan tidak mendapatkan efek jera karena kurangnya aturan yang tegas dan jelas.

Perbedaan penelitian tersebut dengan penelitian yang akan dilakukan oleh penulis terletak pada pembahasanya, jurnal ini berfokus terhadap mengenai penyalahgunaan aplikasi *Deepfake* dan dampaknya terhadap masyarakat, termasuk bentuk-bentuk tindakan penyalahgunaan seperti kejahatan pornografi, pencurian data pribadi, dan penipuan, sedangkan penelitian yang akan dilakukan oleh penulis fokus terhadap kebutuhan mendesak (urgensi) bagi Indonesia untuk meratifikasi Konvensi Budapest, yang merupakan instrumen hukum internasional tentang kejahatan siber, khususnya dalam konteks penyalahgunaan teknologi *deepfake*, dengan pendekatan perspektif *maqashid syariah*

Tabel 1.1

Penelitian Terdahulu

No	Nama/Instansi/ Tahun/Judul	Rumusan Masalah	Hasil	Novelty
1.	Jeremiah Maximillian Laza dan Rizky Karo Karo, Universitas Pelita Harapan Indonesia, 2023, "Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP Dan GDPR"	1.Bagaimana perlindungan hukum terhadap AI Deepfake dalam aspek penyalahgunaannya ditinjau dari General Data Protection Regulation (GDPR)? 2.Bagaimana perlindungan hukum terhadap AI Deepfake dalam aspek penyalahgunaannya ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia?	Pengaturan deepfake dalam GDPR di Eropa dan UU PDP di Indonesia pada dasarnya sudah memberikan perlindungan terhadap data pribadi serta manipulasi informasi digital, meski tidak secara khusus menyebut fenomena deepfake. GDPR menekankan perlindungan data pribadi dari pemrosesan tanpa izin, sedangkan UU PDP menegaskan pertanggungjawaban hukum bagi pelaku penyalahgunaan data, termasuk jika digunakan untuk tindak pidana seperti penipuan atau penyebaran berita bohong. Namun, kedua regulasi ini masih meninggalkan kekosongan karena belum ada aturan spesifik yang mengatur penggunaan teknologi AI dan deepfake secara langsung. Oleh karena itu, dibutuhkan regulasi	Titik kebaruan pada penelitian saya adalah terletak pada integrasi antara analisis *hukum internasional* dan *perspektif maqāṣid al-syarī'ah* dalam meninjau urgensi ratifikasi Konvensi Budapest sebagai upaya pencegahan penyalahgunaan teknologi deepfake di Indonesia.

			yang lebih tajam dan komprehensif untuk menyeimbangkan antara perkembangan inovasi teknologi dan perlindungan hak asasi manusia.	
2.	Muhammad Ariq Abir Jufri dan Akbar Kurnia, Universitas Jambi, 2021, "Aspek Hukum Internasional Dalam Pemanfaatan Teknologi *Deepfake* Terhadap Perlindungan Data Pribadi"	1.Bagaimana aspek-aspek hukum internasional mengatur pemanfaatan Deepfake Technology terkait perlindungan data pribadi? 2.Bagaimana dampak terhadap hukum nasional Indonesia ?	Aspek hukum dalam konteks Hukum Internasional terkait perlindungan data pribadi dapat dilihat melalui instrumen kerja sama global seperti *International Telecommunication Union* (ITU) yang berperan dalam mengatur standar komunikasi dan teknologi. Namun, dampaknya terhadap hukum nasional Indonesia, khususnya dalam perlindungan data pribadi, masih terbatas. Hal ini karena regulasi Indonesia belum sepenuhnya komprehensif dan mengikat dalam mengatur penyalahgunaan teknologi deepfake serta perlindungan data pribadi warganya.	Titik kebaharuan pada penelitian saya adalah spesifik menyoroti urgensi ratifikasi Konvensi Budapest sebagai langkah strategis dalam menghadapi penyalahgunaan *deepfake* di Indonesia, yang sebelumnya belum banyak dikaji. Selain itu, penelitian ini menghadirkan kebaharuan dengan mengintegrasikan perspektif *Maqashid Syariah* pendekatan ini mengaitkan upaya ratifikasi dengan prinsip kemaslahatan umat dan tanggung jawab moral negara
3.	Ermanto Fahamsyah,Vicko Taniady,Kania Venisa Rachim, dan Novi Wahyu Riwayanti,	1.Apa saja problematika yang dihadapi dalam penanganan pelaku cybercrime lintas negara?	Indonesia, cybercrime belum diatur dalam regulasi khusus, namun masih mengacu pada KUHP dan UU ITE. Kedua	Titik kebaharuan pada penelitian saya membahas ratifikasi Konvensi Budapest khusus

	Universitas Jember, 2022, "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention"	2.Bagaimana penerapan prinsip *Aut Dedere Aut Judicare* melalui ratifikasi *Budapest Convention* terhadap pertanggungjawaban pidana bagi pelaku *cybercrime* lintas negara?	aturan ini menghadapi kendala serius, terutama dalam menangani pelaku lintas negara karena masalah yurisdiksi, kedaulatan, dan pembuktian locus delicti yang sering menimbulkan multi yurisdiksi, untuk mengatasinya, diperlukan peran hukum internasional melalui penerapan prinsip *Aut Dedere Aut Judicare*, yang mewajibkan negara untuk mengadili atau mengekstradisi pelaku serta bekerja sama dengan negara lain. Oleh karena itu, ratifikasi *Budapest Convention* menjadi penting sebagai dasar hukum internasional dalam pemberantasan cybercrime.	untuk mencegah penyalahgunaan teknologi *deepfake*, serta menganalisis urgensinya melalui pendekatan maqashid syariah sebagai dasar moral dan hukum Islam.
4.	Meirza Aulia Chairani,Krista Yitawati dan Angga Pramodya Pradhana, Universitas Merdeka Madiun, 2024,"Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake"	1.Apa saja bentuk atau tindakan penyalahgunaan aplikasi Deepfake bagi pelaku tindak pidana? 2.Apa saja ketentuan hukum pidana yang diterapkan pada pelaku penyalahgunaan aplikasi Deepfake bagi pelaku tindak pidana?	*Deepfake* berpotensi disalahgunakan untuk menjatuhkan nama baik tokoh publik, menyebarkan kebencian, maupun membuat konten pornografi dengan menempelkan wajah seseorang ke tubuh pemeran sehingga seolah-olah ia terlibat dalam aktivitas seksual. Tindakan ini kerap dilakukan untuk pemerasan,	Titik kebaruan pada penelitian saya adalah membawa isu penyalahgunaan teknologi *deepfake* ke dalam ranah hukum internasional dengan menempatkan ratifikasi Konvensi Budapest sebagai langkah untuk

			pengancaman, maupun mencelakai korban. Secara hukum, pelaku tindak pidana Deepfake dapat dijerat dengan beberapa aturan, antara lain: UU ITE Pasal 27 ayat (1) jo Pasal 45 ayat (1), UU Pornografi Pasal 4 ayat (1) jo Pasal 29 (pidana 6 bulan – 12 tahun), UU Perlindungan Anak Pasal 4 ayat (1) huruf f jo Pasal 38 (pidana 6 bulan – 6 tahun), UU Perlindungan Data Pribadi (PDP) Pasal 66 jo Pasal 68 (pidana 6 tahun), KUHP baru Pasal 407 (pidana 10 bulan – 10 tahun). Dengan demikian, meskipun belum ada aturan khusus mengenai Deepfake, instrumen hukum yang ada sudah dapat digunakan untuk menjerat pelakunya.	mengatasi keterbatasan regulasi nasional di Indonesia, serta mengintegrasikan perspektif Maqashid Syariah
5.	Chiquita Thefirstly Noerman dan Aji Lukman Ibrahim, Universitas Pembangunan Nasional "Veteran" Jakarta ,2024,	1.Bagaimana pengaturan Mengenai Tindak Pidana Deepfake Di Indonesia ? 2.Bagaimana pengaturan Yang Ideal Mengenai Tindak Pidana	Indonesia saat ini hanya mengatur pemalsuan data pribadi secara umum melalui UU PDP serta pemalsuan secara elektronik dalam UU ITE, yang keduanya merupakan	Titik kebaruan pada penelitian saya adalah secara khusus menyoroti penyalahgunaan teknologi deepfake sebagai bentuk baru

	"Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindung Negara"	*Deepfake* Di Masa Mendatang ?	turunan dari UUD NRI 1945. Namun, aturan khusus mengenai tindak pidana deepfake belum diatur secara eksplisit. Untuk mengantisipasi hal tersebut, Kementerian Komunikasi dan Informatika mendorong adanya regulasi terkait penggunaan deepfake, khususnya dengan kewajiban memberikan penanda bahwa media tersebut telah dimanipulasi.	kejahatan siber (cybercrime) yang menuntut ratifikasi Konvensi Budapest sebagai langkah konkret memperkuat sistem hukum siber Indonesia. Penelitian ini juga menghadirkan perspektif maqashid syariah yang menekankan kewajiban negara dalam menjaga kehormatan (ḥifẓ al-'irḍ), keamanan (ḥifẓ an-nafs), serta stabilitas sosial dan moral masyarakat (ḥifẓ al-maslaha al-'āmmah).

Berdasarkan pemaparan penelitian terdahulu diatas, terdapat banyak perbedaan baik dari segi tujuan objek, serta memiliki titik fokus di masing-masing penelitian. Sehingga dalam penelitian ini, penulis ingin memfokuskan penelitian terhadap urgensier ratifikasi Konvensi Budapest sebagai instrumen hukum internasional dalam mencegah penyalahgunaan teknologi *deepfake* di Indonesia, dengan menggunakan perspektif *maqashid syari*

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum *Deepfake*

Deepfake pertama kali muncul dari seorang pengguna Reddit pada tahun 2017. Ia membuat video palsu dengan wajah selebriti menggunakan teknik *deep learning*. Sejak saat itu, teknologi ini berkembang pesat dan digunakan untuk berbagai keperluan pengetahuan, dengan dampak positif maupun negatif.[56] Menurut Dinas Kominfo Kabupaten Kubu Raya, *deepfake* adalah teknologi berbasis *AI* yang dapat membuat seseorang terlihat atau terdengar melakukan sesuatu yang tidak pernah terjadi.[57]

Deepfake adalah teknologi sintesis media yang menggunakan kecerdasan artifisial (*AI*), terutama teknik pembelajaran mendalam (*deep learning*) untuk membuat konten audio dan visual terlihat dan terdengar seperti asli.[58] "*Deep*" berarti pembelajaran mendalam dalam kecerdasan buatan dan "*fake*" berarti palsu. Secara teknis, *deepfake* sering menggunakan jaringan saraf tiruan seperti *Generative Adversarial Networks* (GAN).[59]

---

[56] Siti Maimunah, "Apa Itu Deepfake?," *INCA University*, 2025, https://inca.ac.id/deepfake/.
[57] Jemi Andartanto, "Apa Itu Deepfake? Kenali Bahaya dan Cara Mendeteksinya," *Dinas Kominfo Kab. Kubu Raya*, 2024, https://kominfo.kuburaya.go.id/apa-itu-deepfake-kenali-bahaya-dan-cara-mendeteksinya.
[58] Robert Chesney dan Danielle K. Citron, "Deep Fakes: A Looming Challenge for Priv Es: A Looming Challenge for Privacy, Democr , Democracy, and National Security," Boston University School of Law, 2020, 1757.
[59] Irma Budiarti, "Apa Itu Deepfake? Ini Bahayanya," Berita, *detiknews.com*, 2025, https://www.detik.com/jatim/berita/d-8090720/apa-itu-deepfake-ini-bahayanya.

Berikut adalah tabel penjelasan terkait *deepfake* dari beberapa litelatur (jurnal):

Tabel 1.2

Penjelasan *Deepfake*

No.	***Deepfake***
1.	*Deepfake* sebuah teknik manipulasi citra, audio, dan video yang sangat realistis dengan menggunakan algoritma pembelajaran mendalam (*deep learning*)[60]
2.	Istilah deepfake berasal dari gabungan kata deep learning, yang merujuk pada teknologi pembelajaran mesin yang mendalam, dan fake, yang berarti palsu. Deepfake merupakan bentuk AI yang dimanfaatkan untuk menghasilkan gambar, video, serta rekaman audio palsu yang tampak realistis dan dapat menipu.[61]
3.	*(Deepfake) this capability makes it possible to create audio and video of real people saying and doing things they never said or did* Kemampuan ini memungkinkan pembuatan audio dan video orang sungguhan yang mengatakan dan melakukan hal-hal yang sebenarnya tidak pernah mereka katakan atau lakukan.[62]
4.	Konten deepfake dapat digunakan untuk berbagai keperluan ilegal atau jahat, mulai dari menyebarkan misinformasi berbahaya, memproduksi pornografi AI tanpa persetujuan, hingga digunakan dalam pencurian atau penipuan skala besar. Teknologi deepfake telah menjadi kekuatan disruptif dalam lanskap digital saat ini. Dengan semakin mudahnya mengakses AI generatif, perangkat

[60] Sri Wahyuni Nurdin dan Imam Fadhil Nugraha, "Ancaman Deepfake Dan Disinformasi Berbasis Ai: Implikasi Terhadap Keamanan Siber Dan Stabilitas Nasional Indonesia," *JIMR: Journal Of International Multidisciplinary Research* vol 4, no. 1 (2025): 74, https://doi.org/10.62668/jimr.v4i01.1551.

[61] Madalaine Christella Seveney dkk., "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi," *Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum sumpah Pemuda* 31, no. 2 (2025): 98, https://doi.org/10.46839/disiplin.v31i2.1167.

[62] Chesney dan Citron, "Deep Fakes: A Looming Challenge for Priv Es: A Looming Challenge for Privacy, Democr , Democracy, and National Security," 1757.

	untuk kloning suara, pertukaran wajah, dan pembuatan media sintetis.
5.	*Deepfake technology, which is based on artificial intelligence to create visual and audio content that is very similar to the original but completely fake, has raised concerns in various sectors, especially in the political context* Teknologi deepfake, yang berbasis pada kecerdasan buatan untuk menciptakan konten visual dan audio yang sangat mirip dengan aslinya tetapi sepenuhnya palsu, telah menimbulkan kekhawatiran di berbagai sektor, terutama dalam konteks politik.[63]
6.	*Deepfakes, a technology that uses sophisticated algorithms to create fake videos, images, or audio that are virtually indistinguishable from the real thing, have changed the face of cybercrime and disinformation.* Deepfake, sebuah teknologi yang menggunakan algoritma canggih untuk membuat video, gambar, atau audio palsu yang hampir tidak dapat dibedakan dari aslinya, telah mengubah wajah kejahatan siber dan disinformasi.[64]
7.	*Deepfake Technology* merupakan algoritma yang memungkinkan penggunanya untuk mengubah wajah dari satu aktor menjadi wajah dari aktor lain dalam video yang berbentuk *photorealistic*.[65]
8.	*Deepfake* merupakan suatu produk dari AI yang menggabungkan, mempersatukan, mengganti dan menempatkan gambar maupun klip video untuk membuat video palsu bisa tampak seperti video itu asli, dan video tersebut dikatakan oleh orang tersebut padahal secara kenyataan orang yang digantikan wajahnya pada video tersebut tidak pernah berkata atau bertindak seperti itu. Teknologi ini bisa menghasilkan seperti contoh video lucu, pornografi ataupun video politik dari seseorang yang mengatakan sesuatu, tanpa

[63] Rofi Aulia Rahman dan Rizaldy Anggriawan, "Deepfake and Election Crimes:Comparative Perspectives from Indonesia,India,Pakistan,and theU.S," *Indonesian Comparative Law Review* vol 7, no. 2 (2025): 132, https://dx.doi.org/10.18196/iclr.v7i2.26337.
[64] Mahrus Ali dkk., "Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims," *Substantive Justice International Journal of Law* 8, no. 1 (2025): 1, https://doi.org/10.56087/substantivejustice.v8i1.306.
[65] Jufri dan Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," 42.

	adanya persetujuan dari orang yang ada di gambar dan suaranya terlibat di dalamnya.[66]
9.	*Deepfake videos are defined as a resulting media from the synthesis of different persons' images and videos mostly faces, replacing a real one.* Video *deepfake* didefinisikan sebagai media hasil sintesis gambar dan video orang yang berbeda sebagian besar wajah, yang menggantikan wajah asli.[67]
10.	*Deepfake technology, powered by AI advancements, threatens digital media integrity and societal trust by creating highly realistic fake videos and audio, making it difficult to distinguish fact from fiction.* Teknologi *deepfake*, yang didukung oleh kemajuan AI, mengancam integritas media digital dan kepercayaan masyarakat dengan menciptakan video dan audio palsu yang sangat realistis, sehingga sulit untuk membedakan fakta dari fiksi.[68]
11.	*Deepfake* adalah teknologi berbasis kecerdasan buatan (AI) yang umum digunakan untuk memalsukan atau memanipulasi foto, video, dan audio dengan menggunakan teknik pemindaian mendalam pada gambar orang menggunakan teknologi.[69]
12.	*Deepfake* merupakan sebuah teknologi yang menggunakan *artificial intelligence* untuk memproduksi atau mengedit suara, foto, maupun video yang sebenarnya tidak pernah terjadi.[70]
13.	*Deepfake* memungkinkan penciptaan konten audio-visual yang sangat menyerupai kenyataan, padahal secara faktual adalah rekayasa.[71]

[66] Laza dan Karo Karo, "Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP dan GDPR [Legal Protection of Artificial Intellegence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR]," 137.
[67] Nikolaos Misirlis dan Harris Bin Munawar, "From Deepfake To Deep-Useful: Risks And Opportunities Through A Systematic Literature Review," International Conferences e-Society, 2022, 26.
[68] Judijanto dkk., "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia," 102.
[69] Arvitto, "Implikasi Hukum Deepfake," 75.
[70] Noerman dan Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara," 604.
[71] Basah dkk., "Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake di Media Sosial," 6.

14.	*Deepfake* memanfaatkan algoritma pembelajaran mendalam untuk mengubah gambar, video, atau suara, sehingga dapat membuat individu tampak melakukan atau mengatakan sesuatu yang sebenarnya tidak pernah terjadi.[72]
15.	*Deepfake* adalah teknik yang memanfaatkan AI untuk membuat, menggabungkan, atau memodifikasi gambar, video, atau audio sehingga tampak seperti asli, padahal merupakan hasil rekayasa.[73]

Berdasarkan tabel tersebut, *deepfake* secara konsisten dipahami sebagai teknologi berbasis kecerdasan buatan, khususnya *deep learning*, yang digunakan untuk memanipulasi atau mensintesis gambar, video, dan audio sehingga menghasilkan konten palsu dengan tingkat realisme yang sangat tinggi. Teknologi ini memungkinkan seseorang tampak mengatakan atau melakukan sesuatu yang sebenarnya tidak pernah terjadi, baik melalui penggantian wajah, suara, maupun penggabungan elemen visual dan audio secara artifisial (rekayasa).

Teknologi *deepfake*, meskipun banyak dikaitkan dengan hal negatif seperti menyebarkan informasi palsu, konten vulgar, dan berita palsu, juga memiliki banyak manfaat positif jika digunakan dengan bijak. Salah satu contohnya adalah dalam dunia pendidikan, di mana pendidik bisa memanfaatkan *deepfake* seakan-akan tokoh sejarah atau ilmuwan terkemuka berbicara langsung kepada audiens untuk memberikan materi

[72] Kartika Ardina Raesyah Putri dkk., "Legal Liability For Using Artificial Intelligence To Produce Deepfakes Under Personal Data Protection Lawpertanggungjawaban Hukum Atas Penggunaan Artificial Intelligenceuntuk Deepfakemenurut Uu Perlindungan Data Pribadi," *Jurnal Rechswetenschap*, 2025, 5, https://doi.org/10.36859/rechtswetenschap.v2i2.3962.
[73] Kristiyenda dkk., "Pencegahan Kejahatan Deepfake," 150.

yang lebih dalam dan menarik.[74] Selain itu, di bidang hiburan dan film, *deepfake* bisa digunakan untuk membuat konten kreatif yang baru dan keren, misalnya mengembalikan kehidupan aktor atau tokoh yang sudah meninggal sebagai bentuk penghormatan atau untuk membuat cerita baru.[75]

Teknologi ini juga bisa digunakan untuk melestarikan budaya, contohnya museum bisa memakai wajah atau suara tokoh budaya yang penting untuk menceritakan sejarah dengan cara yang lebih hidup dan menarik.[76] Salah satu museum di Indonesia yang memakai teknologi ini adalah Museum Cave AI yang berada di Keraton Kasepuhan Cirebon, yang memanfaatkan teknologi AI dan visualisasi modern untuk menghidupkan kembali tokoh sejarah seperti Sultan Matangaji.[77]

---

[74] Muhammad Zaenudin, "Mengenal Teknologi Deepfake, Berikut Manfaat dan Dampak Negatif yang Dapat Ditimbulkan," *kompas.com*, 2024, https://www.kompas.com/tren/read/2024/09/13/084500565/mengenal-teknologi-deepfake-berikut-manfaat-dan-dampak-negatif-yang-dapat?page=all&_gl=1*1qdqlfu*_ga*MjE3NTQwMDg5LjE3NDQzNTk3NDA.*_ga_77DJNQ0227*MTc2Mzk3NDU1MS4xLjAuMTc2Mzk3NDczOC4wLjAuMA..#page2.

[75] Mahfud Febry Styanto, "Potensi Positif Deepfake: Teknologi Sintesis Wajah untuk Edukasi, Perfilman, dan Pelestarian Budaya," *iBenews*, 2025, https://www.ibenews.id/teknologi/2056033315/potensi-positif-deepfake-teknologi-sintesis-wajah-untuk-edukasi-perfilman-dan-pelestarian-budaya.

[76] Styanto, "Potensi Positif Deepfake: Teknologi Sintesis Wajah untuk Edukasi, Perfilman, dan Pelestarian Budaya."

[77] Fathnur Rohman, "Keraton Kasepuhan menghadirkan Museum 'Cave AI' untuk wisata sejarah," *Antara News,* 2024, https://www.antaranews.com/berita/4423793/keraton-kasepuhan-menghadirkan-museum-cave-ai-untuk-wisata-sejarah.

Gambar 1 contoh deep learning dalam ilustrasi wajah Sultan Matangaji

Sumber akun instagram @infokeratonkesapuhan

Dalam industri pemasaran, *deepfake* dapat menurunkan biaya produksi dan meningkatkan personalisasi kampanye. Misalnya, setelah persetujuan diperoleh, iklan dapat dibuat dengan meniru wajah atau suara duta merek tanpa melakukan rekaman ulang.[78] Secara akademis, kajian sistematis terhadap literatur *deepfake* menunjukkan bahwa teknologi ini tidak hanya menimbulkan ancaman tetapi juga memiliki banyak peluang di bidang hiburan, game, pendidikan, dan interaksi publik.[79] Adanya pengaturan dan peraturan yang tepat, *deepfake* dapat menjadi alat transformasi yang memperkaya pengalaman manusia dan bukannya alat untuk manipulasi.

[78] Bernard Yoe, "AI Deepfake : Manfaat atau Bahaya?," *kumparan.com*, 2024, https://kumparan.com/bernardyoe/ai-deepfake-manfaat-atau-bahaya-23jqGNHsLj9.
[79] Misirlis dan Munawar, "From Deepfake To Deep-Useful: Risks And Opportunities Through A Systematic Literature Review," 26–27.

Berbagai peluang tersebut menunjukkan bahwa *deepfake* dapat menjadi teknologi bermanfaat jika digunakan dengan benar, namun praktik di lapangan tidak selalu mudah. Meskipun ada keuntungan besar, ada risiko yang perlu diperhatikan, terutama ketika teknologi ini dibuat dan disebarkan tanpa pengawasan. Berbagai skenario *deepfake* yang sering digunakan, seperti manipulasi *audio*, *real-time audio* dan *video*, serta konten yang sudah direcord, sering menjadi celah penyalahgunaan yang dapat merusak kepercayaan publik dan meningkatkan kemungkinan penipuan digital. Skenario *deepfake* yang biasa digunakan umumnya hanya *audio*, *real-time audio* dan video, *pre-recorded video* dan *audio.*[80]

1. *Audio* : penipu menyamar dengan menggunakan teknologi kloning suara. Mereka melakukan ini dengan melatih model suara untuk meniru nada dan suara seseorang asli dengan benar. Biasanya dalam panggilan telepon langsung, suara kloning digunakan untuk menjawab pertanyaan dan menumbuhkan kepercayaan dengan calon korban. Korban diyakinkan untuk berdonasi ke rekening palsu seolah-olah mereka mendukung organisasi yang sah.
2. *Real-time audio*: penipu menggunakan teknologi *deepfake* untuk membuat umpan video langsung secara real-time di perangkat lunak obrolan video lainnya, menyamar sebagai seseorang.

[80] Abiraam Kesavarajah dkk., "Deepfake Technology Unveiled: The Commoditization of AI and Its Impact on Digital Trust," Cornell University, 2025, 4.

Penipu dapat membuat diri mereka secara visual dan audio mirip dengan seseorang yang sebenarnya dengan menggunakan alat kloning suara bertenaga AI dan sintesis wajah. Tujuan dari komunikasi real-time ini adalah untuk memberikan lapisan kepercayaan kepada korban yang skeptis yang membutuhkan konfirmasi langsung, terutama dalam hal transaksi keuangan yang penting.

3. *Pre-Recorded Video & Audio*: penipu tersebut menggunakan teknologi *deepfake* untuk membuat rekaman video yang menampilkan seseorang yang terkenal atau tokoh siapapun yang diciptakan oleh kecerdasan buatan. Versi kloningan video diunggah ke situs web resmi, dan menggunakan media sosial mereka dapat menipu banyak korban .

Secara global, ruang lingkup *deepfake* telah menjadi sangat luas dan memiliki efek yang sangat kompleks. Teknologi ini memberi kita kesempatan untuk menjadi kreatif dalam industri hiburan, seperti memperbarui adegan dalam film atau menghidupkan kembali aktor yang telah meninggal, di sisi lain *deepfake* telah berkembang menjadi alat yang efektif untuk menyebarkan informasi yang salah dan tidak benar, membuat konten pornografi non-konsensual yang menargetkan individu, dan

melakukan penipuan sosial (*social engineering*) dan penipuan bisnis (seperti pemalsuan suara untuk penipuan finansial).[81]

Deepfake sangat membahayakan kepercayaan masyarakat, integritas informasi, dan keamanan nasional. Kepercayaan yang membentuk interaksi sosial dan demokrasi dapat rusak ketika masyarakat mulai mempertanyakan kebenaran setiap rekaman suara atau video. Oleh karena itu, memahami *deepfake* melibatkan pemahaman lebih dari sekedar teknologi, itu melibatkan pemahaman tentang berbagai ancaman yang dihadapi kebenaran, privasi, dan keamanan di era digital.

B. Tinjauan Umum Konvensi Budapest

Konvensi Budapest dibuat karena kebutuhan mendesak untuk menangani peningkatan kejahatan siber internasional. Sejak pertengahan 1980-an, Dewan Eropa (*Council of Europe*) telah mempertimbangkan solusi pidana untuk masalah teknologi informasi, namun tidak ada instrumen hukum internasional yang lengkap.[82] Konvensi tentang Kejahatan Siber dibuat pada akhir 1980-an sebagai tanggapan atas upaya organisasi untuk memerangi kejahatan siber, yang didasarkan pada keyakinan Dewan bahwa dunia siber yang tanpa batas menuntut solusi yang melampaui batas negara.

Konvensi Kejahatan Siber adalah hasil dari perundingan intensif selama hampir empat tahun antara negara-negara anggota Dewan Eropa,

[81] Yisroel Mirsky, "The Creation and Detection of Deepfakes: A Survey," Georgia Institute of Technology and Ben-Gurion University, 2020, 30.
[82] Council of Europe, "Action against Cybercrime," Digital Governance, *Council of Europe*, 2022, https://www.coe.int/en/web/digital-governance/cybercrime.

Amerika Serikat, Kanada, Jepang, dan negara-negara non-anggota lainnya. Susunannya dimulai pada tahun 1997, dan pada November 2001, Komite Menteri Dewan Eropa mengadopsi teks terakhir. Konvensi ini diresmikan di Budapest, Hongaria, pada tanggal 23 November 2001, dan dikenal sebagai "Konvensi Budapest". Konvensi ini resmi berlaku pada 1 Juli 2004 setelah setidaknya lima negara anggota Dewan Eropa ratifikasinya. Hal ini menandai perkembangan penting dalam cara komunitas internasional menangani kejahatan siber.[83]

Konvensi Budapest tentang Kejahatan Dunia Maya (ETS No. 185) adalah perjanjian internasional pertama yang bertujuan untuk mengatasi kejahatan dunia maya dengan mengatur hukum nasional, meningkatkan teknik investigasi, dan meningkatkan kerjasama internasional.[84] Konvensi ini dibuka untuk penandatanganan di Budapest, Hungaria, pada November 2001, dan terbuka bagi negara-negara anggota dan non-anggota Dewan Eropa. Tujuan utamanya adalah untuk membuat kebijakan kriminal yang komprehensif yang melindungi masyarakat dari kejahatan siber dengan menerapkan peraturan yang seimbang antara kepentingan penegakan hukum dan penghormatan atas hak asasi manusia.[85]

[83] Law Notes, "The Council of Europe's Cybercrime Convention: A Framework for International Cybersecurity," *The Law Institute*, 2023, https://thelaw.institute/regulation-of-cyberspace/council-europe-cybercrime-convention-framework.
[84] "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols."
[85] "Action against Cybercrime," *Council of Europe*, t.t., diakses 9 Mei 2025, https://www.coe.int/en/web/cybercrime.

Pengaturan Konvensi Budapest sangat luas, dan dapat dibagi menjadi empat pilar utama.[86]

Tabel 2.2

Ketentuan Hukum

No	Aspek	Uraian	Rujukan Pasal
1.	Kriminalisasi Kejahatan Siber	Negara wajib mengkriminalisasi pelanggaran kerahasiaan, integritas, dan ketersediaan data/sistem (akses ilegal, intersepsi ilegal, gangguan data), kejahatan komputer (pemalsuan, penipuan), kejahatan konten (pornografi anak), serta pelanggaran hak cipta.	Bab II Pasal 2–10
2.	Alat Penegakan Hukum	Mengatur kewenangan penyidikan seperti penggeledahan dan penyitaan sistem komputer, pembekuan data secara cepat, serta pengumpulan data lalu lintas secara real-time.	Bab II Pasal 16–21
3.	Kerja Sama Internasional	Menyediakan kerangka MLA yang cepat untuk penyelidikan kejahatan siber, termasuk jaringan kontak 24/7 untuk bantuan darurat.	Bab III Pasal 23–35
4.	Penyimpanan & Perlindungan Data	Mengatur mekanisme penyimpanan dan perlindungan data guna menyeimbangkan kebutuhan investigatif dengan perlindungan privasi individu.	Bab II Pasal 15-17

[86] Budapest, "Convention on Cybercrime," European Treaty Series, 2001.

Berdasarkan tabel diatas, pasal yang relevan dengan kejahatan *deepfake* adalah Bab II Pasal 2–10 yang mengatur mengenai kriminalisasi kejahatan siber merupakan bagian yang paling relevan untuk dikaitkan dengan praktik *deepfake*. Pada dasarnya, teknologi *deepfake* bekerja dengan memanipulasi data digital, baik berupa gambar, suara, maupun video. Tindakan ini dalam konteks hukum dapat dikategorikan sebagai *computer-related forgery* (pemalsuan berbasis komputer) maupun *computer-related fraud* (penipuan berbasis komputer), tergantung pada tujuan dan akibat yang ditimbulkannya.

Apabila *deepfake* digunakan untuk menyebarkan informasi yang tidak benar, merusak reputasi seseorang, atau menipu demi memperoleh keuntungan finansial, maka ketentuan mengenai pemalsuan dan penipuan melalui sistem komputer dalam Pasal 2–10 dapat dijadikan dasar hukum yang kuat. Lebih jauh lagi, jika pembuatan *deepfake* tersebut melibatkan akses tanpa hak ke akun, perangkat, atau data pribadi korban, maka unsur *illegal access* maupun *data interference* sebagaimana diatur dalam pasal-pasal tersebut juga berpotensi terpenuhi. Dengan demikian, rangkaian ketentuan dalam Bab II Pasal 2–10 memiliki relevansi langsung dalam menjerat penyalahgunaan teknologi *deepfake*.

Beberapa negara yang telah meratifikasi Konvensi Budapest, antaranya:[87] Albania, Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Belgia, Benin, Bosnia dan Herzegovina, Brasil, Bulgaria, Tanjung Verde, Kamerun, Kanada, Chili, Kolombia, Kosta Rika, Pantai Gading, Kroasia, Siprus, Ceko, Denmark, Republik Dominika, Ekuador, Estonia, Finlandia, Fiji, Prancis, Georgia, Jerman, Ghana, Yunani, Grenada, Hungaria, Islandia, Israel, Italia, Jepang, Kiribati, Latvia, Liechtenstein, Lituania, Luksemburg, Malta, Mauritius, Monako, Montenegro, Maroko, Belanda, Selandia Baru, Nigeria, Makedonia Utara, Norwegia, Panama, Paraguay, Peru, Filipina, Polandia, Portugal, Moldova, Rumania, Rwanda, San Marino, Sao Tome dan Principe, Senegal, Serbia, Sierra Leone, Slovakia, Slovenia, Spanyol, Sri Lanka, Swedia, Swiss, Tonga, Tunisia, Turki, Ukraina, Britania Raya, Amerika Serikat, Vanuatu.

Negara pertama yang meratifikasi Konvensi Budapest adalah Albania pada tahun 2002, disusul 64 negara lainnya.[88] Negara-negara yang meratifikasi Konvensi Budapest memiliki konsekuensi yang jelas. Mereka memperoleh kapasitas yang lebih besar untuk melakukan penegakan hukum siber, yang mencakup akses yang lebih cepat ke kerangka kerja legal lintas-batas dan alat prosedural kontemporer. Selain itu, ditegaskan bahwa negara-negara pihak memperoleh *"effective legal frameworks and procedures to investigate cybercrime and secure electronic evidence"* yaitu kerangka

[87] Strasbourg, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY," *Council of Europe*, 2025, https://www.coe.int/en/web/cybercrime/parties-observers?utm.
[88] "Convention on Cybercrime (ETS No. 185) –," Cybercrime Convention Committee (T-CY), 2020, https://rm.coe.int/09000016809f44f0.

hukum yang efektif dan prosedur untuk menyelidiki *cybercrime* dan melindungi bukti elektronik, serta peningkatan kapasitas untuk menangani bukti digital, harmonisasi hukum nasional, dan percepatan kerja sama internasional melalui jaringan kontak point yang beroperasi 24 jam tiap saat.[89]

Negara-negara yang meratifikasi Konvensi Budapest berfokus pada kebutuhan untuk memiliki kerangka hukum yang konsisten dan efisien untuk menangani kejahatan siber dan mengamankan bukti elektronik. Selain itu, negara meratifikasi konvensi karena menawarkan sarana kerja sama lintas-batas yang cepat dan andal, seperti akses ke bukti elektronik di yurisdiksi luar negeri dan jaringan bantuan darurat 24 jam sehari, yang sangat penting untuk memerangi kejahatan siber modern yang bergerak cepat. Konvensi ini diharapkan untuk meningkatkan kemampuan penegak hukum, meningkatkan keamanan nasional, dan melindungi stabilitas ekonomi digital yang rentan terhadap serangan dan manipulasi teknologi, termasuk penyalahgunaan *deepfake*

C. Teori Tanggung Jawab Negara *(State Responsibility)*

Tokoh dalam pengembangan teori ini adalah James Crawford, yang dikenal melalui karyanya *The International Law Commission's Articles on State Responsibility* (2002) dan *State Responsibility: The General Part* (2013). Dalam kedua karya tersebut, Crawford menguraikan secara

[89] Strasbourg, "The Budapest Convention on Cybercrime: Benefits and Impact in Practice," Cybercrime Convention Committee (T-CY), 2020.

mendalam bahwa kelalaian suatu negara dalam bertindak atau kegagalannya mencegah pelanggaran hukum yang dilakukan oleh pihak di bawah yurisdiksinya, termasuk individu maupun kelompok non-negara, dapat dikategorikan sebagai pelanggaran hukum internasional (*wrongful act*).[90] Teori tanggung jawab negara *(State Responsibility)* merupakan salah satu prinsip utama dalam hukum internasional yang menegaskan bahwa suatu negara dapat dimintai pertanggungjawaban apabila melakukan pelanggaran terhadap kewajiban yang diakui oleh hukum internasional.[91]

Menurut *A Dictionary of Law*, tanggung jawab negara adalah *"The obligation of a state to make reparation arising from a failure to comply with a legal obligation under international law"*[92] artinya Kewajiban suatu negara untuk melakukan reparasi (perbaikan) yang timbul akibat kegagalan untuk mematuhi kewajiban hukum berdasarkan hukum internasional.

Lahirnya teori tanggung jawab negara ini didasari oleh dua teori yaitu, pertama, teori risiko yang berarti bahwa suatu negara bertanggung jawab secara mutlak atas setiap kegiatan yang menghasilkan akibat yang sangat membahayakan, bahkan jika kegiatan itu dianggap sah menurut hukum, kedua teori kesalahan menghasilkan prinsip tanggung jawab subjektif atau tanggung jawab atas dasar kesalahan, yang berarti bahwa negara hanya dapat bertanggung jawab atas tindakannya jika tindakannya

[90] James Crawford, "Tanggung Jawab Negara," 1998.
[91] Martin Dixon dkk., "11. State Responsibility," dalam *Cases & Materials on International Law*, oleh Martin Dixon dkk. (Oxford University Press, 2016), https://doi.org/10.1093/he/9780198727644.003.0011.
[92] Elizabeth A. Martin, "A Dictionary of Law," dalam *Oxford Dictionary of Law*, 5 ed. (Oxford Paperback Reference, 2002), 477.

dapat dibuktikan. Menurut hukum internasional, jenis tanggung jawab negara dapat dibagi menjadi dua diantarnya:[93]

1. Tanggung jawab karena melakukan perbuatan yang melanggar hukum *(delictual liability)*, jenis tanggung jawab ini bisa muncul dari setiap kesalahan atau kelalaian suatu negara terhadap orang asing yang berada di wilayah negara tersebut atau di wilayah negara lain.
    a. Negara yang meluncurkan satelit wajib menanggung seluruh kerugian yang ditimbulkan satelit tersebut terhadap objek milik negara lain. Prinsip yang berlaku adalah tanggung jawab absolut
    b. Eksplorasi nuklir menempatkan negara pada tanggung jawab penuh atas setiap kerusakan yang muncul dari aktivitas tersebut. Prinsip yang dipakai adalah tanggung jawab absolut, jadi upaya pencegahan sebelumnya tidak memengaruhi kewajiban negara, sehingga negara tetap memikul tanggung jawab apa pun yang terjadi.
    c. Negara wajib mengatur dan mengawasi semua aktivitas di wilayahnya, termasuk yang berdampak lintas batas dan berpotensi merugikan negara lain. Jenis tanggung jawab ditentukan oleh karakter kegiatannya. Jika aktivitas itu menimbulkan bahaya serius, negara memikul tanggung jawab mutlak. Kegiatan yang bersifat umum atau tidak berbahaya, tanggung jawab negara bergantung

[93] Billy Diego Arli Papilaya dkk., "Tanggung Jawab Negara Terhadap Pelanggaran Hak Asasi Manusia Di Belarusia Ditinjau Dari Hukum Internasional," *Tatohi Jurnal Ilmu Hukum* vol 1, no. 6 (2021): 536–37.

pada ada tidaknya kelalaian atau kesengajaan dalam tindakan tersebut.

2. Tanggung jawab dalam pelanggaran perjanjian *(contractual liability)* negara juga memikul tanggung jawab internasional ketika melanggar perjanjian yang telah disepakati. Kewajiban ini muncul saat negara gagal memenuhi komitmen kontraktualnya dan menimbulkan pelanggaran terhadap perjanjian tersebut.

Negara bertanggung jawab atas tindakan yang melanggar hukum, sehingga setiap kelalaian yang menyebabkan kerugian yang melintasi batas negara tetap memerlukan pertanggungjawaban secara penuh, dengan tanggung jawab yang melanggar hukum *(delictual liability)*. Penyalahgunaan *deepfake* muncul dari aktivitas digital yang melintasi batas negara, dan hal ini jelas membutuhkan pengaturan yang ketat. Negara mempunyai kewajiban untuk mengawasi ruang siber dan memastikan bahwa semua aktivitas di wilayah hukumnya tidak merugikan negara lain atau warganya sendiri. Ketika ancaman semakin serius, seperti manipulasi data , pencurian identitas , atau perusakan reputasi karena *deepfake*, prinsip tanggung jawab negara mengarah pada kewajiban yang lebih tegas. Pentingnya penerapan Konvensi Budapest menjadi sangat jelas tanpa standar internasional yang mengikat, pengawasan nasional tidak akan seimbang, dan risiko negara tidak bertindak tepat waktu dalam mengatasi penyalahgunaan *deepfake* semakin besar.

Crawford menjelaskan bahwa tanggung jawab suatu negara tidak hanya berkaitan dengan norma primer yang mengatur perilaku negara, seperti larangan agresi dan perlindungan hak asasi manusia, tetapi juga mencakup bagaimana negara tersebut harus bertanggung jawab di tingkat internasional ketika norma-norma primer tersebut dilanggar. Berdasarkan laporan ILC, ia membedakan secara tegas antara *primary rules* yang berisi kewajiban substansial dan *secondary rules* yang mengatur konsekuensi atas pelanggaran kewajiban tersebut.[94] Tanggung jawab internasional suatu negara timbul apabila terdapat tindakan yang dapat diatribusikan kepada negara dan melanggar kewajiban internasional yang dimilikinya.

Crawford menjelaskan bahwa terdapat dua unsur utama yang harus terpenuhi agar suatu negara dapat dinyatakan bertanggung jawab, yakni pertama, adanya perbuatan yang dapat diatribusikan kepada negara, baik dilakukan oleh organ negara maupun oleh individu atau entitas yang menjalankan kekuasaan negara, kedua, adanya pelanggaran terhadap kewajiban internasional yang berlaku bagi negara tersebut, kemudian ia juga menguraikan berbagai syarat atribusi yang mencakup tindakan organ negara, pelaksanaan fungsi pemerintahan oleh entitas tertentu, serta adanya kontrol atau pengarahan negara terhadap tindakan tersebut.[95]

Teori Crawford menegaskan bahwa prinsip *due diligence* mewajibkan setiap negara untuk memastikan wilayah serta infrastrukturnya

[94] James Crawford, "First Report on State Responsibility, by Mr. James Crawford," Legal UN, 1998.
[95] James Crawford, "The International Law Comission's Articles On State Responbility," Cambridge University Press, 2002, 91 & 124.

tidak dimanfaatkan bagi kegiatan yang dapat merugikan negara lain atau melanggar norma hukum internasional. Apabila suatu negara telah mengetahui adanya potensi pelanggaran namun tidak melakukan tindakan pencegahan, kondisi tersebut dapat dikategorikan sebagai bentuk kelalaian (*omission*).[96]

Menurut Kerangka Tanggung Jawab Negara, yang diuraikan oleh Crawford, negara bertanggung jawab tidak hanya atas tindakan aparaturnya sendiri, tetapi juga atas kegagalan mencegah tindakan berbahaya yang terjadi di bawah yurisdiksinya, termasuk yang bersifat digital dan lintas batas. Prinsip *due diligence* menuntut negara untuk memastikan bahwa infrastruktur dan wilayahnya tidak menjadi tempat pelanggaran yang merugikan negara lain atau warganya sendiri.[97] Indonesia sendiri kurangnya peraturan komprehensif tentang penggunaan AI dan belum diratifikasinya Konvensi Budapest menunjukkan adanya celah besar dalam pemenuhan tanggung jawab preventif tersebut. Indonesia tidak memiliki perangkat hukum domestik dan standar internasional yang cukup untuk mendeteksi, mencegah, dan menindak penyalahgunaan teknologi seperti *deepfake* lintas yurisdiksi, karena keterlambatan ini. Perspektif tanggung jawab negara, kurangnya ratifikasi dan peraturan dapat ditafsirkan sebagai kelalaian

[96] Ian Yuying Liu, "State Responsibility and Cyberattacks: Defining Due Diligence Obligations 4(2) The Indonesian Journal of International and Comparative Law 191-260," *The Indonesian Journal of International & Comparative Law*, 2017, 193.
[97] Richard Mackenzie-Gray Scott, "Due Diligence as a Secondary Rule of General International Law," *Leiden Journal of International Law* 34, no. 2 (2021): 344, https://doi.org/10.1017/S0922156521000030.

negara dalam memenuhi kewajiban *due diligence*, terutama dalam menghadapi ancaman kejahatan siber berbasis AI yang semakin berbahaya.

D. *Maqashid Syariah*

Maqashid al-Syari'ah tersusun dari dua istilah, yaitu *maqashid* dan *al-syari'ah*. Kata *maqashid* merupakan bentuk jamak dari *maqshid* atau *maqshad*, yang berasal dari kata kerja *qashada–yaqshudu*. Secara etimologis, istilah tersebut memiliki beragam makna, namun dalam konteks pembahasan ini diartikan sebagai tujuan dari hukum.[98] Secara terminologis, *maqashid* merujuk pada maksud dan hikmah yang ditetapkan Allah SWT di balik setiap hukum-hukumNya. *Syariah* secara bahasa berarti jalan menuju sumber air, yang dapat dimaknai sebagai jalan menuju kebahagiaan. Berdasarkan hal tersebut, *maqashid al-syari'ah* dipahami sebagai tujuan-tujuan dari syariat Islam yang terkandung dalam setiap ketentuan dan aturan yang telah ditetapkan oleh Allah SWT.[99]

Menurut Ibnu Asyur arti *maqashid al-Syariah* secara keseluruhan (*maqashid al-syariah al-'ammah*). Ibnu Asyur mencontohkan hal-hal seperti menjaga ketertiban umum, menegakkan keadilan, menolak dampak negatif, dan lain-lain. Selain itu, Ibnu Asyur memberikan definisi khusus untuk arti *maqashid al-Syariah* yaitu "Syari' menetapkan berbagai langkah yang bertujuan menghadirkan manfaat bagi manusia serta menjaga

[98] Sutisna dkk., *Panorama Maqashid* (Media Sains Indonesia, 2021), 52.
[99] *panorama Maqashid Syariah*, 53.

kemaslahatan mereka, baik dalam kehidupan umum maupun tindakan khusus yang mereka lakukan.[100]

Menurut Nurdin bin Mukhtar al-Khadimi menyimpulkan bahwa *maqashid al-syariah* adalah "*Maqaṣid al-syariah* pada hakikatnya mencerminkan tujuan hukum yang dikehendaki Allah, yaitu menghadirkan kemaslahatan dalam setiap ketentuan syar'i. Kemaslahatan itu tampak, misalnya, dalam ibadah puasa yang membentuk ketakwaan, dalam jihad yang berfungsi menghadapi ancaman dan melindungi masyarakat, serta dalam pernikahan yang menjaga pandangan, memelihara kehormatan, mempertahankan keberlanjutan keturunan, dan menghidupkan peradaban di bumi Allah."[101]

Konsep *Maqasid Syariah* merupakan salah satu prinsip dasar yang sangat penting dalam ajaran Islam yang menekankan bahwa syariat Islam hadir untuk mewujudkan serta menjaga kemaslahatan bagi umat manusia. Tujuan utama *Maqasid Syariah* adalah menciptakan kebaikan dan mencegah keburukan, atau dengan kata lain, menarik manfaat dan menolak kemudaratan (*dar'u al-mafasid wa jalb al-masalih*).[102] Menurut Imam Al-Ghazali, maqashid syariah merupakan upaya untuk mencapai tujuan pengabdian dengan cara mencegah segala bentuk kemudaratan serta

[100] Muhamad Rezi dkk., "Al-Maqâshid Al-Syarî'ah ; Teori dan Implementasi," *Sahaja Journal Sharia And Humanities* vol 2, no. 1 (2023): 159.
[101] Rezi dkk., "Al-Maqâshid Al-Syarî'ah ; Teori dan Implementasi."
[102] Paryadi, "Maqashid Syariah : Definisi Dan Pendapat Para Ulama," 206.

mengusahakan tercapainya kemaslahatan. Prinsip ini dikenal dengan sebagai dasar dalam mendapatkan kebaikan dan menolak kerusakan.[103]

Imam Ghazali membagi menjadi 5 yang disebut sebagai *al-mabaadi al-khamsyah* :[104]

1. Perlindungan terhadap agama (*hifzd al-din*)
2. Menjaga jiwa (*hifzd al-nafs*)
3. Menjaga akal (*hifzd –'aql*)
4. Menjaga keturunan (*hifdz al-nasl*), dan
5. Menjaga harta (*hifzd al-maal*)

Penggunaan teknologi *deepfake* untuk tujuan penipuan, fitnah, atau pencemaran nama baik berpotensi mengancam *ḥifẓ al-'aql* karena menyesatkan akal masyarakat melalui informasi palsu, mengganggu *ḥifẓ al-nafs* karena menimbulkan tekanan psikologis dan kerugian bagi korban, merusak *ḥifẓ al-nasl* karena dapat mencederai kehormatan keluarga serta keturunan, dan mengancam *ḥifẓ al-māl* karena menyebabkan kerugian ekonomi.

Ratifikasi Konvensi Budapest menjadi bentuk upaya negara dalam menerapkan prinsip *dar' al-mafāsid wa jalb al-maṣāliḥ*, yaitu mencegah kerusakan dan mewujudkan kemaslahatan melalui penyesuaian hukum nasional dengan standar internasional guna melindungi masyarakat dari ancaman kejahatan digital masa kini.

[103] Paryadi, "Maqashid Syariah : Definisi Dan Pendapat Para Ulama," 208.
[104] Tanza Dona Pertiwi dan Sri Herianingrum, "Menggali Konsep Maqashid Syariah: Perspektif Pemikiran Tokoh Islam," *Jurnal Ilmiah Ekonomi Islam* Vol 10, no. 1 (2024): 814.

BAB III

PEMBAHASAN

A. Urgensitas Ratifikasi Konvensi Budapest di Indonesia

Kemajuan teknologi kecerdasan buatan, terutama *deepfake*, telah melahirkan kategori baru ancaman terhadap keamanan informasi dan stabilitas nasional Indonesia. Teknologi *deepfake* memiliki kemampuan untuk menghasilkan konten audio-visual yang sangat realistis dan sangat menantang untuk dibedakan dari peristiwa aktual, sehingga memfasilitasi penyebaran disinformasi, manipulasi sentimen publik, dan serangan terhadap legitimasi lembaga pemerintah.[105] Menurut data *We Are Social & Meltwater* di Indonesia penggunaan internet mencapai 212 juta orang pada awal tahun 2025, ketika presentase online mencapai 74,6 persen.[106] Kondisi ini menunjukkan bahwa ruang digital Indonesia semakin padat dan terbuka, sehingga penyebaran konten manipulatif seperti *deepfake* meningkat secara signifikan karena jangkauan distribusinya yang semakin luas dan sulit dikendalikan.

Struktur pemerintah Indonesia menempatkan negara dalam peran tanggung jawab penuh, bertugas menjaga hak-hak konstitusional warga negara baik di ranah fisik maupun digital. Tugas ini jelas diartikulasikan dalam Pasal 28G ayat (1) UUD NRI 1945, yang menegaskan bahwa "setiap

[105] Nurdin dan Nugraha, "Ancaman Deepfake Dan Disinformasi Berbasis Ai: Implikasi Terhadap Keamanan Siber Dan Stabilitas Nasional Indonesia."
[106] Simon Kemp, "Digital 2025: Indonesia," *wearesocial.com*, 2025, https://datareportal.com/reports/digital-2025-indonesia.

orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya."[107] Hak-hak ini melayani fungsi pertahanan dan perlindungan, menyiratkan bahwa negara tidak hanya dilarang melakukan pelanggaran tetapi juga diharuskan untuk secara proaktif melindungi masyarakat dari campur tangan orang lain, termasuk pelanggaran yang digerakkan oleh teknologi seperti *deepfake* yang merusak kehormatan, harga diri, dan keselamatan pribadi.

Perlindungan tersebut dijelaskan lebih lanjut dalam Pasal 28F Undang-Undang Dasar NRI 1945, yang menegaskan bahwa semua individu memiliki hak untuk memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi. Penegasan ini menyiratkan bahwa pemerintah dipaksa untuk menjamin bahwa informasi yang beredar dalam ranah digital beroperasi dalam kerangka hukum yang aman dan akuntabel, di sinilah letak korelasi yang jelas antara hak-hak konstitusional dan tanggung jawab negara untuk menjaga integritas lingkungan informasi publik.[108] Penyediaan perlindungan negara yang tidak memadai terhadap eksploitasi teknologi *deepfake* melampaui kekurangan teknis belaka dalam infrastruktur digital dapat ditafsirkan sebagai pelanggaran kewajiban konstitusional untuk melindungi warga negara.

---

[107] Ira Apriyanti, "The Urgency of Establishing Personal Data Protection Act and Financial Technology Act in Digital Era in Order to Protect and Control the Privacy in Indonesia," *Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019)*, 2020, 345, https://doi.org/10.2991/aebmr.k.200321.045.

[108] Adam Muhshi, "Pemenuhan Hak atas Informasi Publik sebagai Tanggung Jawab Negara dalam rangka Mewujudkan Good Governance," *Lentera Hukum* vol 5, no. 1 (2020): 64, https://doi.org/10.19184/ejlh.v5i1.7284.

Penafsiran konstitusi sejalan dengan prinsip kewajiban positif negara *(positive obligations of the state)*, yang menegaskan bahwa pemerintah tidak hanya diharuskan untuk menahan diri dari pelanggaran hak asasi manusia tetapi juga memiliki kewajiban untuk menerapkan tindakan pencegahan dan hukuman terhadap ancaman yang ditimbulkan oleh aktor non-negara.[109] Penyalahgunaan *deepfake* adalah karakteristik serangan oleh aktor non-negara yang memanfaatkan kekurangan peraturan dan teknologi.

Regulasi nasional saat ini selain UUD NRI 1945 yaitu Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Indonesia masih gagal menangani masalah yang ditimbulkan oleh teknologi *deepfake*. Salah satu masalah utama adalah kedua undang-undang ini tidak memberikan definisi yang jelas tentang *deepfake*.[110] Meskipun Undang-Undang ITE mengatur manipulasi dan penyebaran informasi elektronik palsu dan Undang-Undang PDP mengatur perlindungan data pribadi secara keseluruhan, tidak ada peraturan yang mendefinisikan atau mengatur *deepfake* secara khusus.[111] Penggunaan teknologi *deepfake* di Indonesia membutuhkan reformasi

[109] Marija Jovanovic, "Positive Obligations as a Means of Establishing State Responsibility for 'Modern Slavery' in Human Rights Law," dalam *State Responsibility for 'Modern Slavery' in Human Rights Law*, 1 ed., oleh Marija Jovanovic (Oxford University PressOxford, 2023), 95, https://doi.org/10.1093/oso/9780192867087.003.0005.
[110] Muhammad Doing dkk., "Legal Challenges In Combating Deepfake Abuse: A Comparative Studyof Ai Regulation In Privacy Protection And Digital Security," *International Conference Restructuring and Transforming Law 2* vol 4, no. 1 (2025): 638.
[111] Arvitto, "Implikasi Hukum Deepfake," 79.

undang-undang yang lebih adaptif dan responsif untuk mengimbangi perkembangan teknologi.

Peraturan perundang-undangan seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), harus diperbarui dengan memberikan definisi yang jelas tentang *deepfake*, menggunakan metode forensik digital untuk meningkatkan penegakan hukum, dan menetapkan tanggung jawab yang jelas bagi platform digital.[112] Kekosongan hukum ini menyebabkan perlindungan konstitusional yang tidak memadai, karena struktur hukum saat ini gagal mengatasi ancaman yang muncul yang secara langsung mempengaruhi perlindungan reputasi, informasi pribadi, dan keamanan data.[113]

Ketika peraturan tentang perlindungan data pribadi, keamanan siber, dan tata kelola konten digital gagal mengatasi ancaman yang muncul seperti penyalahgunaan *deepfake*, maka perlindungan konstitusional mungkin dianggap tidak memadai secara operasional. Kurangnya peraturan tentang *deepfake* yang jelas menyebabkan penegak hukum berjuang untuk memahami penafsiran pasal, kualifikasi tindak pidana dan alasan pembuktian karena *deepfake* tidak seperti penyalinan gambar biasa, dokumen palsu, atau pencemaran nama baik. Akibatnya, mereka yang

[112] Doing dkk., "Legal Challenges In Combating Deepfake Abuse: A Comparative Studyof Ai Regulation In Privacy Protection And Digital Security," 644.
[113] Russel Butarbutar, "Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia," International Conference on Law and Governance, 2019, 155.

terkena dampak tidak menerima perlindungan yang memadai, sementara pelanggar menikmati celah teknologi yang memungkinkan mereka menghindari konsekuensi.

Seluruh masalah ini tidak dapat dipisahkan dari teori Tanggung Jawab Negara sesuai James Crawford. Crawford mengklaim bahwa suatu negara bertanggung jawab tidak hanya atas tindakan langsungnya, tetapi juga untuk kelalaiannya *(omission)* ketika tidak mencegah pelanggaran hukum internasional oleh individu di bawah kendalinya.[114] Prinsip *due diligince* mewajibkan negara untuk menjamin bahwa wilayah, infrastruktur, dan jaringan digital mereka tidak dieksploitasi untuk melancarkan serangan terhadap negara lain atau warganya.[115] Indonesia, yang tidak memiliki peraturan khusus tentang *deepfake*, belum menyelaraskan undang-undang cybernya dan belum terlibat dalam kerangka kerja sama internasional, membuatnya rentan untuk dilihat gagal menjunjung tinggi kewajiban *due diligince* ini.

James Crawford, dalam *The ILC Articles on State Responsibility* (2002), menyatakan bahwa suatu negara dapat dimintakan pertanggungjawaban tidak hanya ketika pejabat atau organnya melakukan pelanggaran hukum internasional, tetapi juga ketika negara gagal mencegah tindakan yang seharusnya dihindari dengan standar *due diligince* yang

[114] Crawford, "Tanggung Jawab Negara."
[115] Neil Mcdonald, "The Role Of Due Diligence In International Law," *Cambridge University Press for the British Institute of International and Comparative Law*, 2020, 1042.

sesuai.[116] Intinya, meningkatnya masalah penyalahgunaan *deepfake* yang melampaui lintas batas tidak hanya mewakili masalah kejahatan siber, tetapi juga cerminan dari komitmen suatu negara untuk menegakkan tanggung jawab internasionalnya dalam menjaga wilayah, sistem, dan infrastrukturnya agar tidak dieksploitasi untuk tindakan yang membahayakan negara lain atau penduduknya sendiri.

Sudut pandang tanggung jawab *delictual liability*, suatu negara dapat dilihat sebagai lalai jika menyadari ancaman namun gagal menerapkan langkah-langkah hukum yang tepat untuk mengurangi dampaknya.[117] Negara-negara memiliki tanggung jawab untuk mencegah tindakan yang mengarah pada bahaya lintas batas, termasuk yang ada di ranah digital. Jika negara lain menderita karena *deepfake* yang berasal dari Indonesia, atau jika individu Indonesia menjadi korban pelanggar asing sementara Indonesia tidak memiliki mekanisme kerja sama, kelalaian ini dapat dilihat sebagai pelanggaran tanggung jawab internasional.

Deepfake merupakan kejahatan yang sulit untuk dipantau tanpa bantuan dari negara lain, dan bukti digital dapat menghilang dengan cepat. Informasi dapat diubah, server dapat dipindahkan, dan rekaman dapat dihapus dalam beberapa saat. Konvensi Budapest secara khusus menguraikan prosedur untuk pelestarian data komputer yang disimpan cepat

[116] Federica Paddeu dan Christian J. Tams, "Encoding the law of State responsibility with courage and resolve: James Crawford and the 2001 Articles on State Responsibility," *Cambridge International Law Journal* 11, no. 1 (2022): 3–4, https://doi.org/10.4337/cilj.2022.01.01.
[117] Faculty of Law, International Vision University dkk., "Cyber Warfare And International Criminal Law: State Responsibility For Cyber Attacks," *Congress Proceedings*, 24 Oktober 2024, 197, https://doi.org/10.55843/ISC2024conf189n.

(Pasal 16) dan pelestarian yang dipercepat dan pengungkapan sebagian data lalu lintas (Pasal 17).[118]

Ratifikasi Konvensi Budapest menjadi urgen bagi Indonesia karena karakter lintas-batas dari ancaman *deepfake* menuntut mekanisme kerja sama hukum pidana internasional yang efektif.[119] Pada dasarnya, *deepfake* memanfaatkan infrastruktur dan layanan yang seringkali tersebar di berbagai yurisdiksi, seperti server hosting, platform distribusi, penyedia layanan cloud, atau penyedia teknologi generatif.[120] Karena itu, menangani *deepfake* hanya di ranah domestik dapat menghadapi masalah prosedural seperti permintaan bantuan hukum yang lama, ketidakmampuan untuk memantau bukti elektronik, atau perbedaan definisi tindak pidana antar negara.

Konvensi Budapest dibuat untuk menyelaraskan standar materiil dan prosedural penegakan kejahatan siber, seperti pengamanan, pengumpulan bukti elektronik, dan bantuan hukum dan ekstradisi yang mempercepat penanganan kasus dengan pihak lintas negara.[121] Oleh karena itu, tidak meratifikasi konvensi ini akan menghambat kemampuan Indonesia untuk meminta dan memberikan bantuan cepat ketika bukti *deepfake* ditemukan di luar negeri.

---

[118] "Convention on Cybercrime."
[119] Strasbourg, "The Budapest Convention on Cybercrime: Benefits and Impact in Practice."
[120] Europol, "Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers," EUROJUST, 2024, https://www.eurojust.europa.eu/sites/default/files/assets/trans-border-access-to-stored-computer-data-under-article-32-of-the-budapest-convention-on-cybercrime-and-extraterritorial-powers-23-01-2024.pdf.
[121] Helaine Leggat, "A New Look at the Budapest Convention on Cybercrime," *ITCL*, t.t., diakses 3 Desember 2025, https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/.

Ratifikasi Konvensi Budapest tidak bertentangan dengan kerangka hukum nasional Indonesia karena struktur kenegaraan telah menetapkan proses pembuatan, persetujuan dan pelaksanaan perjanjian internasional melalui Undang-Undang No. 24 tahun 2000 tentang Perjanjian Internasional. Pasal 9 dan 10 menetapkan bahwa perjanjian internasional yang berkaitan dengan masalah politik, perdamaian, pertahanan keamanan, perubahan teritorial, kedaulatan, atau hak asasi manusia perlu disetujui oleh undang-undang, bukan hanya dengan perintah presiden.

Konstitusi tidak menyebutkan bahwa instrumen hukum internasional bertentangan dengan prinsip kedaulatan negara.[122] Secara khusus, Pasal 28I paragraf (4) UUD NRI 1945 menekankan bahwa negara memiliki tanggung jawab dalam melindungi hak asasi manusia, sementara Konvensi Budapest berfungsi sebagai alat hukum internasional yang meningkatkan kapasitas negara untuk memenuhi kewajiban ini di ranah digital.

Bahkan pernyataan Direktur Jenderal Aplikasi TIK Kementerian Komunikasi dan Informatika Republik Indonesia dalam forum internasional bapak Ashwin Sasongko yang dilaksanakan pada tanggal 23-25 Maret 2010 di Strasbourg, Prancis beliau menyatakan bahwa Indonesia perlu ratifikasi

[122] Hikmahanto Juwana, "Hukum Internasional Sebagai Instrumen Politik: Beberapa Pengalaman Indonesia Sebagai Studi Kasus," *Arena Hukum* 5, no. 2 (2012): 106, https://doi.org/10.21776/ub.arenahukum.2012.00502.4.

konvensi budapest tentang kejahatan siber. Tujuan utama indonesia untuk meratifikasi konvensi ini adalah:[123]

1. Untuk menyelesaikan undang-undang tentang informasi dan transaksi elektronik, baik hukum substantif maupun prosedural
2. Untuk meningkatkan kerja sama internasional dalam menangani kegiatan kejahatan siber, hal-hal tersebut penting dalam melindungi warga negara, keamanan dan kepentingan negara
3. Meningkatkan hubungan dan kerja sama dengan organisasi internasional dan masyarakat internasional.

Pernyataan yang dibuat oleh Direktur Jenderal Aplikasi TIK dari Kementerian Komunikasi dan Informatika Indonesia pada sebuah forum internasional di Strasbourg menyoroti bahwa Indonesia telah mengakui pentingnya meningkatkan kerangka hukumnya dan berkolaborasi secara global untuk memerangi kejahatan dunia maya sejak awal. Penekanan pada perlunya meratifikasi Konvensi Budapest melampaui sekadar mengikuti perkembangan teknologi ini menandakan kebutuhan penting Indonesia untuk meningkatkan hukum nasionalnya mengenai informasi dan transaksi elektronik sambil mengatasi tantangan yurisdiksi terkait kejahatan siber internasional. Dengan menggunakan ratifikasi sebagai sarana untuk meningkatkan kolaborasi internasional dan diplomasi hukum, Indonesia bertujuan untuk melindungi warga negara dan kepentingan nasional

[123] Ashwin Sasongko, "General Remaks The Director General Of Ict Application Ministry Of Communication And Information Technology Republic Of Indonesia 23 - 25 March, 2010, Strasbourg, France," conference paper presented pada Octopus Interface Conference, Perancis, 2010.

sekaligus memperkuat perannya sebagai anggota komunitas global yang berkomitmen dalam memastikan keamanan siber di seluruh dunia.

Kebutuhan untuk meratifikasi Konvensi Budapest menjadi semakin jelas, terutama terkait dengan penyalahgunaan teknologi *deepfake* di Indonesia. Salah satu contoh kasus penyalahgunaan *deepfake* di Indonesia yang menggemparkan adalah beredarnya video manipulatif yang menampilkan tokoh politik Prabowo Subianto. Rekaman video tersebut, Prabowo tampak mengenakan pakaian batik dan menyampaikan pernyataan seolah-olah ia telah resmi menjadi Presiden Indonesia dan akan memberikan bantuan sebesar 50 juta rupiah kepada setiap warga negara. Video itu disisipi dengan tayangan lain yang menunjukkan seseorang tengah menghitung uang menggunakan mesin, sehingga menimbulkan kesan seolah-olah ucapan tersebut benar-benar otentik. Padahal, video tersebut adalah hasil rekayasa digital berbasis *deepfake* yang dirancang untuk menyesatkan publik dan memanipulasi persepsi masyarakat.[124] Kasus ini menyoroti ancaman signifikan yang ditimbulkan oleh penyalahgunaan teknologi *deepfake*, yang merugikan reputasi orang dan juga dapat mengganggu stabilitas sosial dan politik negara.

Kasus lainnya yang tidak kalah menggemparkan ialah kasus *deepfake* yang mencuat pada bulan April 2025 adalah tiga tersangka kasus penipuan *deepfake* yang dimana pelaku memanipulasi video dan audio tiga gubernur dari Pulau Jawa. Tiga video editan tersebut menggunakan *AI*, para

[124] Kristiyenda dkk., "Pencegahan Kejahatan Deepfake," 160.

tersangka mengubah narasi dan suara tiga gubernur yaitu Gubernur Jatim Khofifah Indar Parawansa, Gubernur Jateng Ahmad Luthfi, dan Gubernur Jabar Dedi Mulyadi yang mengajak untuk segera membeli sepeda motor. Rekaman video tersebut, para gubernur seolah-olah menawarkan sepeda motor dengan harga murah melalui media sosial, padahal itu adalah rekayasa untuk menipu masyarakat agar mentransfer sejumlah uang ke rekening yang telah disiapkan oleh pelaku.[125]

Menteri Keuangan Sri Mulyani juga menjadi salah satu korban penyalahgunaan teknologi *deepfake,* yakni konten hoaks yang dibuat melalui manipulasi berbasis kecerdasan buatan (*AI*). Video tersebut diunggah oleh sebuah akun Instagram dan menampilkan seolah-olah pernyataan tertentu berasal dari dirinya. Organisasi Masyarakat Antifitnah Indonesia (Mafindo) kemudian memastikan bahwa video tersebut bukanlah konten asli, melainkan hasil rekayasa digital yang dibuat menggunakan teknologi Google Veo. Co-Founder sekaligus Fact-Check Specialist Mafindo, Aribowo Sasmito, menjelaskan bahwa pada bagian kanan bawah video terlihat watermark bertuliskan "Veo", yang menjadi indikator bahwa video tersebut dihasilkan melalui platform tersebut.[126]

Berikut merupakan tabel yang menyajikan ringkasan mengenai dua kasus penyalahgunaan teknologi *deepfake* sebagai bentuk ilustrasi terhadap dampak negatif penerapan teknologi tersebut.

---

[125] Rabiah, "Polda Jatim Ungkap Penipuan Deepfake 3 Gubernur Jualan Motor."
[126] Tim Cek Fakta, "Sri Mulyani Korban Deepfake, Bagaimana Deteksi dan Antisipasi Video Palsu?," *KBR*, 2025, https://kbr.id/articles/indeks/sri-mulyani-korban-deepfake-bagaimana-deteksi-dan-antisipasi-video-palsu-.

Tabel 1.3

Kasus *deepfake* di Indonesia

No	Korban / tokoh yang disalahgunakan	Kasus/ bentuk deepfake	Peraturan yang dilanggar	Dampak yang ditimbulkan
1.	Prabowo Subianto	Video deepfake yang menampilkan Prabowo mengenakan batik dan menyampaikan pernyataan palsu seolah-olah telah menjadi Presiden Indonesia dan akan memberikan bantuan Rp50 juta per warga. Video disisipi adegan orang menghitung uang untuk menimbulkan kesan asli	- UU No. 11 Tahun 2008 tentang ITE Pasal 28 ayat (1) tentang penyebaran berita bohong yang menyesatkan publik. Pasal 27 ayat (3) tentang pencemaran nama baik melalui media elektronik. -KUHP Pasal 310 dan 311 (jika terbukti ada unsur fitnah atau pencemaran nama baik).	Tindakan tersebut berpotensi merusak citra serta kredibilitas politik Prabowo, menimbulkan kesesatan informasi di tengah masyarakat, serta dapat mengakibatkan terganggunya stabilitas sosial dan politik pada tingkat nasional.
2.	Gubernur Khofifah Indar Parawansa (Jatim), Ahmad Luthfi (Jateng), dan Dedi Mulyadi (Jabar)	Video deepfake yang memanipulasi wajah dan suara ketiga gubernur untuk mengajak masyarakat membeli sepeda motor murah, dengan tujuan menipu korban agar mentransfer	-UU ITE Pasal 28 ayat (1) tentang berita bohong yang merugikan konsumen atau masyarakat. Pasal 35 tentang manipulasi data elektronik untuk keuntungan pribadi. -KUHP Pasal 378 tentang tindak pidana penipuan.	Fenomena tersebut menyebabkan kerugian ekonomi bagi masyarakat, menurunkan kepercayaan publik terhadap pejabat pemerintah, serta menunjukkan lemahnya mekanisme verifikasi dan deteksi

		uang ke rekening pelaku		konten digital berbasis AI.
3.	Sri Mulyani	Video deepfake yang memperlihatkan Menteri Keuangan Sri Mulyani Indrawati seolah-olah sedang menyampaikan pernyataan bernada provokatif terkait kebijakan ekonomi nasional.	-UU Nomor 1 Tahun 2024, unsur dan ancaman pidananya sebagai berikut: Pasal 27A terkait penyerangan kehormatan atau nama baik secara elektronik. Sanksi pidana diatur dalam Pasal 45 ayat (4) berupa penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp400 juta. Pasal 45 ayat (6) terkait tuduhan yang tidak dapat dibuktikan kebenarannya (fitnah). Ancama sanksi berupa penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750 juta. Pasal 28 ayat (3) terkait penyebaran pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat. Ancama yang diatur Pasal 45A ayat (3) berupa pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1 miliar	Narasi palsu memicu emosi, terutama di kalangan guru, sebelum ada klarifikasi resmi. Publik menjadi ragu terhadap pernyataan asli maupun klarifikasi.

Serangkaian insiden penyalahgunaan *deepfake* di Indonesia menggambarkan bahwa teknologi kecerdasan buatan telah beralih dari inovasi netral menjadi alat nyata dan signifikan untuk kejahatan dunia maya. *Deepfake* digunakan tidak hanya untuk menodai reputasi tokoh publik dan

mempengaruhi opini publik, tetapi mereka juga secara langsung digunakan untuk melakukan penipuan ekonomi yang menimbulkan kerugian nyata pada warga.[127]

Karakteristik bersama dari manipulasi audio-visual yang digerakkan oleh *AI*, penyebaran cepat melalui platform digital, dan potensi pelaku untuk beroperasi lintas batas menunjukkan bahwa kejahatan terkait *deepfake* memiliki aspek transnasional yang tidak dapat ditangani secara memadai hanya melalui kerangka hukum nasional.

Bahaya yang ditimbulkan oleh *deepfake* terhadap keamanan nasional telah menyebabkan negara-negara maju untuk menciptakan teknologi deteksi otomatis, termasuk sistem verifikasi berbasis *AI*, dan untuk mendorong kerja sama internasional dalam memerangi penyalahgunaan *deepfake*.[128] Meskipun video *deepfake* berhasil menyesatkan orang-orang secara langsung, bahaya utama mereka justru terletak pada kemampuan ini ialah menimbulkan ketidakpastian mengenai kebenaran informasi. Ketika masyarakat tidak yakin tentang keaslian video, kepercayaan pada media, institusi, dan bahkan keseluruhan realitas digital dapat dirusak. Teknologi *deepfake* dalam hal ini berfungsi sebagai instrumen disinformasi yang sangat kuat, karena mampu menanamkan

[127] Yang Meliana, "Urgensi Formulasi Perlindungan Hukum Dan Kepastian Pidana Terhadap Pengaturan Tindak Pidana Deepfake Dalam Sistem Hukum Pidana Nasional The Urgency Of Formulating Legal Protection And Criminal Law Certainty Regarding The Regulation Of Deepfake Crimes Within The Indonesian Criminal Law System," *Rewang Rencang : Jurnal Hukum Lex Generalis* vol 6, no. 7 (2025): 2–3.

[128] Olivia Le Poidevin, "UN Report Urges Stronger Measures to Detect AI-Driven Deepfakes," *Reuters*, 2025, https://www.reuters.com/business/un-report-urges-stronger-measures-detect-ai-driven-deepfakes-2025-07-11/.

keraguan daripada hanya menyebarkan kepalsuan. Ketidakpastian ini memicu efek berjenjang yang ditandai dengan berkurangnya kepercayaan pada kerangka politik, hasil pemilihan, dan tokoh publik, yang pada akhirnya mempengaruhi stabilitas pemerintahan demokratis.[129]

Teknologi *deepfake* memungkinkan perubahan yang sangat realistis dari kemiripan visual dan suara seseorang ini telah terbukti menjadi metode untuk kejahatan seperti pornografi non-konsensual, penipuan, fitnah, dan pelanggaran privasi.[130] Oleh karena itu urgensi Indonesia untuk meratifikasi menjadi semakin jelas karena Konvensi Budapest mencakup aspek substantif dan prosedural seperti pelestarian cepat data komputer yang disimpan, melacak lalu lintas digital, mengumpulkan bukti elektronik yang sah secara hukum, ekstradisi, dan bantuan hukum timbal balik (MLA).[131]

B. Analisis Pengaturan *Deepfake*

1. Pengaturan *Deepfake* di Indonesia

Secara spesifik, Indonesia belum memiliki undang-undang atau peraturan pemerintah yang secara eksplisit menyebut dan mengatur khusus tentang teknologi *deepfake*. Pengaturannya masih tersebar dan diinterpretasikan dari beberapa pasal dalam peraturan perundang-undangan yang ada, yang seringkali tidak dirancang untuk menangani

[129] Nurdin dan Nugraha, "Ancaman Deepfake Dan Disinformasi Berbasis Ai: Implikasi Terhadap Keamanan Siber Dan Stabilitas Nasional Indonesia," 82.
[130] SIP Corp, "Deepfake Crimes in Indonesia: Legal Challenges and Criminal Liability in the AI Era," *SIP LAW FIRM*, 2025, https://siplawfirm.id/deepfake-crimes-in-indonesia/.
[131] Committee of Ministers, "Council of Europe modernises provisions for mutual assistance in criminal matters," *Council of Europe*, 2025, https://www.coe.int/en/web/portal/-/council-of-europe-modernises-provisions-for-mutual-assistance-in-criminal-matters.

kompleksitas dan keunikan manipulasi media berbasis AI.[132] Secara konseptual kurangnya pengaturan yang secara khusus ditujukan untuk mengatasi teknologi *deepfake* menempatkan Indonesia dalam sikap reaktif dan bukan proaktif mengenai ancaman yang ditimbulkan oleh manipulasi media yang didorong oleh kecerdasan buatan.

Konteks *deepfake* tersebut, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan UU Nomor 1 Tahun 2024 menjadi instrumen hukum utama yang sementara digunakan untuk menjerat penyalahgunaan *deepfake* dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) juga memiliki relevansi signifikan dalam konteks *deepfake*, khususnya ketika teknologi ini menggunakan wajah, suara, atau identitas seseorang tanpa persetujuan.

a. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang ITE awalnya diberlakukan pada tahun 2008 untuk mengatasi persyaratan hukum yang berasal dari kemajuan pesat teknologi informasi dan transaksi elektronik. Undang-undang ini dianggap penting untuk memberikan kejelasan hukum dan keamanan dalam penggunaan teknologi digital, yang mencakup perlindungan transaksi elektronik dan informasi yang dibuat secara digital. Kebutuhan akan peraturan ini muncul karena teknologi

[132] Seveney dkk., "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi," 99.

digital telah menjadi sesuatu yang penting dalam kehidupan sehari-hari masyarakat dan interaksi bisnis dalam ekonomi digital.[133]

Undang-Undang ITE kemudian direvisi pertama kali pada tahun 2016 melalui Undang-Undang Nomor 19 Tahun 2016 untuk memperbaiki sejumlah norma dan respons terhadap kasus-kasus yang dinilai menunjukkan bahwa aturan awal belum cukup efektif.[134] Pada tanggal 5 Desember 2023 undang-undang ITE terbaru mendapat persetujuan resmi dari DPR dan ditandatangani menjadi undang-undang oleh Presiden Joko Widodo pada 2 Januari 2024, menjadi Undang-Undang No. 1 tahun 2024. Undang-undang ini kemudian mulai berlaku sebagai kerangka hukum baru untuk informasi dan transaksi elektronik di Indonesia.[135]

Berawal dari keadaan ini, tidak adanya peraturan khusus mengenai *deepfake* tidak berarti bahwa Indonesia sama sekali tidak memiliki alat hukum. Praktik penegakan hukum saat ini menunjukkan bahwa pemerintah terus memanfaatkan kerangka hukum yang ada, khususnya Undang-Undang Informasi dan Transaksi Elektronik untuk mengatasi berbagai contoh penyalahgunaan teknologi digital. Undang-Undang ITE kemudian

[133] Samuel Abrijani Pangerapan, "Naskah Akademik Rancangan Undang-Undang Tentang Perubahan Kedua Atas Undangundang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," Kementerian Komunikasi dan Informatika, 2021.
[134] Josua Sitompul, "Wajah Baru UU ITE," *kompas.com*, 2024, https://nasional.kompas.com/read/2024/01/05/06000061/wajah-baru-uu-ite?page=all.
[135] Eva Safitri, "Diteken Jokowi, Revisi UU ITE Jilid II Resmi Berlaku," *detiknews.com*, 2024, https://news.detik.com/berita/d-7123630/diteken-jokowi-revisi-uu-ite-jilid-ii-resmi-berlaku.

telah diposisikan sebagai kerangka hukum utama yang ditafsirkan secara luas untuk mencakup tindakan yang melibatkan manipulasi konten berbasis kecerdasan buatan, seperti *deepfake*, meskipun undang-undang ini awalnya tidak dibuat untuk mengatasi masalah ini secara khusus. Sehubungan dengan teknologi *deepfake* beberapa pasal Undang-Undang ITE memang dapat digunakan secara terbatas. Beberapa pasal Undang-Undang ITE Undang-Undang No. 19 Tahun 2016 sebagaimana diubah dengan Undang-Undang No. 1 Tahun 2024 menjadi landasan utama penanganan konten ilegal di ruang digital, termasuk potensi *deepfake* yang bisa digunakan:

1) Pasal 27 ayat (1): "Setiap Orang dengan sengaja dan tanpa hak menyiarkan,mempertunjukkan,mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum". Pasal ini menjelaskan tentang melanggar kesusilaan. Pasal ini dapat digunakan untuk mengatasi masalah pornografi yang tidak berizin yang dibuat oleh teknologi *deepfake*, yang menonjol sebagai bentuk eksploitasi yang signifikan. Informasi dari *Southeast Asia Freedom of Expression Network* (SafeNet) menunjukkan bahwa sebagian besar insiden *deepfake* di Indonesia melibatkan manipulasi wajah perempuan untuk

konten dewasa, yang secara terang-terangan melanggar martabat dan privasi para korban.[136]

2) Pasal 27A: "Setiap Orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik". Pasal ini menjelaskan tentang menyerang kehormatan atau nama baik. Relevansi pasal ini dengan kasus *deepfake* ialah bahwa *deepfake* bisa digunakan untuk merendahkan, memfitnah, atau mencemarkan nama baik seseorang dapat dijerat dengan pasal ini.
3) Pasal 28 ayat (1): "Setiap Orang dengan sengaja dan/atau mentransmisikan Informasi Elektronik dan/ atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel". Pasal ini menjelaskan tentang penyebaran berita bohong dan menyesatkan. Pasal ini bisa digunakan pada kasus *deepfake* dikarenakan *deepfake* bisa digunakan sebagai alat disinformasi atau hoaks. Laporan Kementerian Komunikasi dan Informatika

[136] Aliya R. Putri, "Bahaya Laten Deepfake: Wajah Diganti, Realitas Dipalsukan," *kumparan.com*, 2025, https://kumparan.com/kumparannews/bahaya-laten-deepfake-wajah-diganti-realitas-dipalsukan-24WchNJRUkJ/.

(Kominfo) kejahatan siber dengan memproduksi konten hoaks dan disinformasi, termasuk diantaranya konten *deepfake*.[137]

4) Pasal 28 ayat (2): "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut, mengajak, atau memengaruhi orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik". Pasal ini menjelaskan tentang permusuhan berdasarkan SARA. Pasal ini bisa dikaitkan dengan kasus *deepfake* dikarenakan *deepfake* memiliki potensi untuk menjadi instrumen yang sangat berpengaruh untuk menghasut perselisihan sosial dengan mengubah dialog atau visual yang menargetkan komunitas tertentu.

Berikut pasal-pasal apabila dirumuskan dalam bentuk tabel:

[137] Nezar Patria, "Deepfake Jadi Modus Kejahatan Siber Baru, Wamen Nezar Tegaskan Pentingnya Mitigasi Risiko," *KOMDIGI*, 2025, https://www.komdigi.go.id/berita/siaran-pers/detail/deepfake-jadi-modus-kejahatan-siber-baru-wamen-nezar-tegaskan-pentingnya-mitigasi-risiko.

Tabel 2.3

Keterkaitan pasal-pasal UU ITE dengan potensi penyalahgunaan teknologi *deepfake*

Pasal	Substansi Pengaturan	Fokus Larangan	Korelasi dengan *Deepfake*
Pasal 27 ayat (1)	Larangan mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik bermuatan pelanggaran kesusilaan	Pelanggaran kesusilaan dan pornografi	*Deepfake* digunakan untuk membuat konten pornografi tidak berizin terutama manipulasi wajah korban yang melanggar martabat, privasi, dan kesusilaan publik
Pasal 27A	Larangan menyerang kehormatan atau nama baik dengan menuduhkan suatu hal melalui media elektronik	Pencemaran nama baik dan penghinaan	*Deepfake* dapat merekayasa pernyataan, perilaku, atau visual palsu yang merendahkan atau memfitnah seseorang sehingga mencederai reputasi korban
Pasal 28 ayat (1)	Larangan penyebaran informasi bohong atau menyesatkan yang mengakibatkan kerugian materiel	Hoaks dan disinformasi	*Deepfake* berfungsi sebagai instrumen disinformasi yang sangat persuasif, digunakan untuk penipuan, manipulasi

			opini publik, atau kejahatan berbasis informasi palsu
Pasal 28 ayat (2)	Larangan penyebaran informasi yang menghasut kebencian atau permusuhan berbasis SARA	Ujaran kebencian dan konflik sosial	*Deepfake* berpotensi dimanfaatkan untuk memprovokasi kebencian dan konflik horizontal dengan merekayasa narasi visual atau audio yang menargetkan kelompok tertentu

Perlu digaris bawahi bahwasanya walaupun UU ITE memiliki beberapa pasal yang mungkin relevan dalam penggunaan *deepfake*, akan tetapi Undang-Undang ITE memiliki kelemahan, yaitu bersifat *technology-neutral* mengenai teknologi dan gagal mempertimbangkan bagaimana AI secara khusus beroperasi. Selain itu, penegak hukum biasanya gagal mengikuti kecepatan penyebaran teknologi, kemudian risiko utama belum tentu berhasil dalam memulihkan kerugian bagi korban (reparasi) atau dalam menghentikan munculnya *deepfake* dari terjadi sejak awal.

b. Undang-Undang Perlindungan Data Pribadi (UU PDP)

Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia dibentuk karena meningkatnya insiden penyalahgunaan

data pribadi di tengah era digital. Munculnya Internet dan kemajuan teknologi informasi, mengakses data pribadi menjadi lebih mudah, namun juga meningkatkan kemungkinan pelanggaran dan penyalahgunaan data. Pemerintah mengakui pentingnya menjaga hak privasi warganya dengan menetapkan peraturan tentang pengumpulan, penyimpanan, dan penggunaan data pribadi. Undang-Undang PDP bertujuan untuk meningkatkan perlindungan data pribadi individu secara lebih baik.[138]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan peraturan yang penting. Pembuatan *deepfake* biasanya membutuhkan penanganan data pribadi biometrik (seperti wajah dan suara) yang termasuk dalam klasifikasi data sensitif sebagaimana dinyatakan dalam Pasal 4. Undang-undang PDP mengakui bahwa informasi biometrik seperti foto wajah dianggap sebagai data pribadi spesifik, yang berarti bahwa menggunakan gambar atau video seseorang tanpa izin mereka dapat dilihat sebagai pelanggaran data pribadi. Namun, pada kenyataannya, undang-undang ini memiliki kekurangan yang signifikan dalam hal menangani *deepfake*.[139]

[138] Mira Sibera, "Memahami UU PDP: Pelindungan Data Pribadi di Indonesia," *SiberMate*, 2024, https://sibermate.com/hrmi/memahami-uu-pdp-pelindungan-data-pribadi-di-indonesia.
[139] Savana Maulia dan Sidi Ahyar Wiraguna, "Penyalahgunaan Foto Berbasis AI Dan Tantangan Hukum Berdasarkan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Jurnal Hukum dan Kewarganegaraan* vol 12, no. 3 (2025): 3, https://doi.org/10.3783/causa.v12i3.12778.

Beberapa alasannya ialah teknologi *deepfake* mencakup mengubah gambar melalui AI, itulah sebabnya Undang-Undang PDP tidak dibuat untuk mengatasi perubahan pasca-pemrosesan seperti swap wajah, pengeditan video, atau penataan ulang gambar.[140] Kesulitan penegak hukum dalam mengidentifikasi para pelaku kebanyakan kasus *deepfake*, identitas pelaku sulit diungkap, serta sulit membuktikan unsur kesalahan *(mens rea)* dalam sistem *AI* yang sulit. Ini menimbulkan kekosongan hukum terkait pertanggungjawaban pidana.[141] Undang-Undang PDP juga tidak menjelaskan definisi atau pedoman yang jelas mengenai konten *deepfake*, Undang-Undang PDP hanya mencakup data pribadi, bukan konten yang menipu atau manipulasi audio-visual.[142]

Dengan demikian, meskipun Undang-Undang PDP menetapkan struktur hukum mendasar untuk melindungi data pribadi, regulasi tersebut gagal sepenuhnya mengatasi kesenjangan hukum yang diciptakan oleh penyalahgunaan teknologi *deepfake*.

c. Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial

Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial

[140] Maulia dan Wiraguna, "Penyalahgunaan Foto Berbasis AI Dan Tantangan Hukum Berdasarkan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi," 9.
[141] Putri dkk., "Legal Liability For Using Artificial Intelligence To Produce Deepfakes Under Personal Data Protection Lawpertanggungjawaban Hukum Atas Penggunaan Artificial Intelligenceuntuk Deepfakemenurut UU Perlindungan Data Pribadi."
[142] Arvitto, "Implikasi Hukum Deepfake," 75.

merupakan pedoman resmi yang diterbitkan oleh Kementerian Komunikasi dan Informatika (Kominfo) pada 19 Desember 2023 sebagai respons atas pesatnya perkembangan dan pemanfaatan teknologi kecerdasan buatan (*artificial intelligence/AI*) di Indonesia. Surat edaran ini ditujukan kepada pelaku usaha yang menjalankan aktivitas pemrograman berbasis *AI* serta penyelenggara sistem elektronik, baik di sektor publik maupun privat, sebagai acuan nilai dan prinsip etika dalam proses pengembangan dan penggunaan teknologi kecerdasan buatan.[143]

Tujuan utama surat edaran ini adalah memberikan pedoman mengenai nilai-nilai etika yang perlu diperhatikan dalam proses pengembangan dan penerapan kecerdasan buatan.[144] Selain itu, surat edaran ini dimaksudkan untuk mendorong pelaku industri serta penyelenggara sistem elektronik agar menerapkan nilai-nilai etika tersebut ke dalam kebijakan internal maupun praktik pemrograman yang mereka jalankan

[143] Dinda Buana Putri, "Kominfo Resmi Terbitkan Surat Edaran Menteri Tentang Etika Kecerdasan Buatan Atau Artificial Intelligent," *VOI*, 2023, https://voi.id/teknologi/341605/kominfo-resmi-terbitkan-surat-edaran-menteri-tentang-etika-kecerdasan-buatan-atau-artificial-intelligent.
[144] Fajar El Pradianto, "Pemanfaatan Teknologi AI Kudu Perhatikan Etika," *RM.id*, 2023, https://rm.id/baca-berita/government-action/203115/se-no92023-terbit-pemanfaatan-teknologi-ai-kudu-perhatikan-etika?

Surat edaran ini mencakup nilai-nilai etika dalam penggunaan teknologi *AI*, diantaranya:[145]

1) Inklusivitas

   Nilai ini menekankan bahwa pemanfaatan kecerdasan buatan harus berlandaskan prinsip kesetaraan, keadilan, dan perdamaian. Oleh karena itu, setiap informasi maupun inovasi yang dihasilkan melalui penggunaan *AI* seharusnya dapat diakses dan dimanfaatkan oleh seluruh lapisan masyarakat, serta diarahkan untuk kepentingan bersama, bukan hanya kelompok atau pihak tertentu.

2) Transparansi

   Prinsip ini menuntut agar pemanfaatan *AI* didasarkan pada keterbukaan, khususnya terkait data yang digunakan dalam proses pengembangannya. Transparansi menjadi penting untuk memastikan bahwa data tersebut diperoleh dan digunakan secara tepat, sehingga dapat mencegah terjadinya penyalahgunaan data dalam pengembangan inovasi teknologi.

3) Kemanusiaan

   Nilai ini menegaskan bahwa pemanfaatan teknologi kecerdasan buatan tidak boleh mengesampingkan aspek kemanusiaan. Penggunaan *AI* harus tetap menghormati dan melindungi hak

[145] Pujiati, "Peraturan yang Mengatur Tentang Artificial Intelligence," *deepublish*, 2025, https://penerbitdeepublish.com/peraturan-yang-mengatur-tentang-artificial-intelligence/.

asasi manusia, menjaga kualitas hubungan sosial dalam masyarakat, menghargai kepercayaan yang dianut, serta tidak meniadakan kebebasan setiap individu dalam menyampaikan pendapat.

4) Keamanan

Aspek keamanan ini mencakup upaya menjaga kerahasiaan dan data pribadi, melindungi privasi pengguna, serta menjamin pemenuhan hak-hak pengguna Sistem Elektronik, dengan demikian pemanfaatan teknologi *AI* tidak menimbulkan kerugian bagi pihak mana pun.

5) Aksesibilitas

Prinsip ini menekankan bahwa pemanfaatan teknologi kecerdasan buatan ditujukan untuk seluruh lapisan masyarakat tanpa pengecualian. Teknologi AI tidak boleh dibatasi hanya untuk kelompok atau kalangan tertentu, melainkan harus dapat diakses secara luas dan setara dan penerapannya harus memastikan tidak adanya praktik atau dampak yang bersifat diskriminatif.

6) Kredibilitas dan Akuntabilitas

Nilai ini menekankan bahwa penggunaan kecerdasan buatan harus berorientasi pada kemampuan pengambilan keputusan yang bersumber dari informasi maupun inovasi yang dihasilkan dan setiap informasi yang diperoleh melalui *AI* tidak dapat

diterima begitu saja, melainkan harus dapat dipertanggungjawabkan oleh pengguna.

7) Perlindungan Data Pribadi

   Prinsip ini menegaskan bahwa setiap pemanfaatan AI harus disertai dengan upaya menjaga keamanan dan kerahasiaan data pribadi, serta dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

8) Pembangunan dan Lingkungan Berkelanjutan

   Nilai ini menegaskan bahwa pemanfaatan kecerdasan artifisial tidak dapat dilepaskan dari pertimbangan dampaknya, baik terhadap manusia, lingkungan, maupun makhluk hidup lainnya

9) Kekayaan Intelektual

   Pemanfaatan kecerdasan artifisial tidak boleh mengabaikan perlindungan hak kekayaan intelektual. Setiap penggunaan *AI* harus dilakukan dengan tetap mematuhi ketentuan peraturan perundang-undangan yang mengatur hak tersebut.

Surat ini dalam konteks penyalahgunaan *deepfake* konten yang direkayasa menggunakan *AI* untuk menampilkan seseorang melakukan atau mengatakan sesuatu yang tidak pernah terjadi belum secara spesifik menjelaskannya. Surat edaran ini hanya ditujukan pada tiga kelompok, yaitu: pelaku usaha aktivitas pemrograman berbasis *AI* pada kode baku lapangan usaha Indonesia 62015, penyelenggara sistem elektronik (PSE) lingkup publik dan

penyelenggara sistem elektronik lingkup privat. [146] Sementara dalam kasus *deepfake* sering kali berasal dari pelaku individu atau kelompok illegal yang menggunakan aplikasi atau model *AI* yang mudah diakses bukan dari pelaku usaha yang terdaftar.

Kelamahan lainnya dari surat edaran ini adalah bahwa surat ini tidak mengikat secara hukum. Menurut Direktur Jenderal Informasi dan Komunikasi Publik (Dirjen IKP) Kemenkominfo Usman Kansong mengatakan, surat edaran terkait etika *AI* tidak mengikat secara hukum dan tidak ada sanksi (bagi pelanggar).[147] Surat edaran ini bergantung pada penerapan peraturan lain yang sudah ada seperti Undang-Undang Informasi dan Transaksi Elektronik atau Undang-Undang Perlindungan Data Pribadi untuk proses hukum bila terjadi pelanggaran nyata dalam praktik.[148]

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP) pada dasarnya mengatur perbuatan yang bersifat umum, seperti penyebaran informasi palsu, pencemaran nama baik, dan pelanggaran terhadap data pribadi , namun kedua undang-undang

[146] Felina Evangelica Setiawan, "Surat Edaran Menkominfo Tentang Etika AI: Apa dan Mengapa?," *Visiniaga*, 2025, https://www.visiniaga.com/blog/our-blog-1/surat-edaran-menkominfo-tentang-etika-ai-apa-dan-mengapa-108?

[147] Diva Lufiana Putri, "Isi SE Menkominfo soal Etika Penggunaan AI, Pelaku Tunduk UU ITE dan UU PDP," *kompas.com*, 2023, https://amp.kompas.com/tren/read/2023/12/23/110000665/index.html?

[148] Galuh Putri Riyanto, "Kominfo Terbitkan SE yang Atur Etika Penggunaan AI," *kompas.com*, 2023, https://tekno.kompas.com/read/2023/12/22/15520497/kominfo-terbitkan-se-yang-atur-etika-penggunaan-ai.

tersebut belum secara tegas mendefinisikan maupun mengkualifikasikan *deepfake* sebagai tindak pidana tersendiri yang memperhitungkan karakteristik khusus teknologi kecerdasan artifisial, seperti proses sintesis, manipulasi konten, dan replikasi identitas tanpa persetujuan.

Akibatnya, aparat penegak hukum kerap dipaksa menerapkan ketentuan yang bersifat umum terhadap fenomena yang pada dasarnya tidak dirancang untuk menjangkau perkembangan teknologi berbasis *AI*. Kondisi ini berpotensi menimbulkan ketidakpastian hukum serta praktik penegakan hukum yang berbeda-beda dalam menangani kasus penyalahgunaan deepfake.

Kurangnya aturan yang jelas tentang *deepfake* menunjukkan bahwa sistem hukum Indonesia masih belum sepenuhnya berkembang dan tidak dapat secara efektif melindungi terhadap bahaya yang ditimbulkan oleh konten yang dimanipulasi yang dibuat melalui kecerdasan buatan.[149] Oleh karena itu, ada kebutuhan untuk perencanaan peraturan sehingga pendekatan hukum terhadap *deepfake* dapat proaktif, menghukum, dan beradaptasi dengan perubahan teknologi.

Tindakan awal ialah harus menetapkan definisi hukum *deepfake* sebagai jenis perubahan konten audio-visual yang

[149] Rahman dan Anggriawan, "Deepfake and Election Crimes:Comparative Perspectives from Indonesia,India,Pakistan,and theU.S."

diproduksi oleh sistem AI. Ambiguitas definisi ini membuat penegak hukum kesulitan untuk mengkategorikan tindakan kriminal, seperti yang ditunjukkan dalam beberapa kasus yang pada akhirnya hanya termasuk dalam ketentuan umum dalam Undang-Undang ITE karena tidak adanya norma khusus yang menangani teknologi ini sebagai kegiatan ilegal.[150]

Indonesia harus membangun kerangka hukum yang khusus dengan mengubah Undang-Undang ITE atau membuat undang-undang baru yang berfokus pada kecerdasan buatan *(AI)*. Berbagai studi penelitian menunjukkan bahwa Undang-Undang ITE dan Undang-Undang PDP gagal menangani secara memadai elemen manipulatif, real-time, dan lintas batas yang terkait dengan *deepfake*. Undang-Undang PDP semata-mata melindungi data pribadi tetapi tidak memiliki pedoman konkret mengenai pembuatan konten sintetis yang dibuat tanpa persetujuan, sementara Undang-Undang ITE hanya membahas hasil seperti pencemaran nama baik, bukan proses memproduksi deepfake itu sendiri.[151] Oleh sebab itu, peraturan baru harus memasukkan aturan yang melarang pembuatan, pengunggahan, distribusi, dan pemanfaatan *deepfake* tanpa persetujuan individu yang identitasnya telah diubah.

[150] Risno dkk., "Pertanggungjawaban Pidana Terhadap Pelaku Deepfake Pornograph," *Jurnal Tana Mana* vol 6, no. 3 (2025): 186, https://doi.org/10.33648/jtm.v6i3.1320.
[151] Hazmin Sulton Firdaus dan Lona Puspita, "Peran Hukum Dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital," *UIR Law Review* vol 9, no. 1 (2025): 5–6.

Mencakup ranah internasional salah satu langkah yang dapat diambil adalah dengan meratatifikasi dan mengadopsi Konvensi Budapest, *deepfake* adalah kejahatan ilegal yang tersebar di seluruh negara, dan untuk mengatasinya membutuhkan kerjasama antar negara.[152] Ratifikasi Konvensi Budapest merupakan langkah penting karena menetapkan proses resmi untuk berbagi bukti elektronik, mengekstradisi tersangka, dan melakukan investigasi digital di berbagai yurisdiksi.[153] Jika Indonesia tidak meratifikasi ini, Indonesia akan kesulitan untuk mengejar penjahat yang menggunakan server asing atau menyembunyikan identitas online mereka dengan *AI*.

2. Pengaturan *Deepfake* di Italia

Italia merupakan pelopor di Eropa dalam mulai mengkriminalkan dan mengatur penyalahgunaan *deepfake*.[154] Pada sidang tanggal 17 September 2025, Senat Italia menyetujui Rancangan Undang-Undang No. 1146-B, yang berjudul "*Provisions and delegated powers to the Government regarding artificial intelligence".* Teks tersebut diterbitkan dalam Jurnal Resmi Italia sebagai Undang-Undang No. 132 tahun 2025 *(Law No. 132 of 2025)* dan akan mulai berlaku pada tanggal 10 Oktober

[152] Yudo Agnastio Nugraha, "Implementasi Konvensi Budapest (2001) Dalam Penanganan Kejahatan Siber" (Universitas Lampung, 2025), 18.
[153] Jansen Chandra dkk., "Peran Interpol dalam Menangani dan Menanggulangi KejahatanSiber di Indonesia," *PESHUM : Jurnal Pendidikan, Sosial dan Humaniora* vol 4, no. 3 (2025): 4711.
[154] Karolina Mania, "Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study," *Trauma, Violence, & Abuse* 25, no. 1 (2024): 122, https://doi.org/10.1177/15248380221143772.

2025.[155] Diberlakukannya Undang-Undang No. 132 tahun 2025, yang mencakup ketentuan dan otorisasi untuk pemerintah mengenai kecerdasan buatan, Italia akhirnya menetapkan kerangka peraturan yang diperbarui untuk mengatasi salah satu penyalahgunaan digital paling berbahaya di era AI yaitu *deepfake*.[156]

Pengaturan tentang *deepfake* secara substantif diatur dalam Bab V Pasal 26 undang-undang tersebut memasukkan Pasal 612-quater yang memperkenalkan delik baru berjudul "*"illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale"* (penyebaran konten yang tidak sah yang dihasilkan atau diubah dengan sistem kecerdasan buatan). Secara keseluruhan bunyi pasalnya "*Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa*" (Siapa pun yang menyebabkan kerugian yang tidak dapat dibenarkan kepada seseorang dengan menyediakan, menerbitkan, atau menyebarluaskan, tanpa persetujuan mereka, gambar, video, atau suara yang dipalsukan atau diubah melalui penggunaan

[155] Andrew Ma, "Italy passes its own law on artificial intelligence: new rules effective October 2025," *The AI Forum Exploring the legal and social challenges of AI*, 2025, https://www.theaiforum.org/news-were-reading/italy-passes-first-national-ai-law.
[156] Sarzana, "New Cybercrimes," *Attorney At Law*, 2025, https://www.lidis.it/en/i-nuovi-reati-informatici.

sistem kecerdasan buatan dan mampu menyesatkan mengenai keasliannya, dapat dihukum dengan penjara selama satu hingga lima tahun. Kejahatan ini dapat dihukum atas pengaduan dari pihak yang dirugikan).[157]

Teks Pasal 612-quater kejahatan baru ini menghukum siapa pun yang**,** tanpa persetujuan orang yang diwakili , menyebarluaskan gambar, video, atau suara yang diubah atau dihasilkan oleh AI dengan cara yang menyesatkan mengenai keasliannya dan menyebabkan kerugian yang tidak adil bagi korban. Undang-undang tersebut menetapkan bahwa siapa pun yang melakukan tindakan tersebut dapat dihukum dengan penjara satu hingga lima tahun . Kejahatan ini dapat dituntut berdasarkan pengaduan dari pihak yang dirugikan, tetapi penuntutan dimulai secara otomatis jika tindakan tersebut:[158]

a. Hal itu terkait dengan kejahatan yang dapat dituntut secara hukum
b. Pelanggaran terjadi terhadap individu yang secara hukum tidak dapat menyetujui (seperti anak-anak atau individu dengan penyakit)
c. Tindak pidana ini dilakukan terhadap otoritas publik karena fungsi yang dijalankannya

Ketentuan ini bertujuan untuk mengisi celah regulasi hingga tahun 2025, individu yang menjadi korban *deepfake* hanya dapat

[157] Luana Giangregorio, "Il nuovo reato di Deepfake (Legge 132/2025)," *IUSTLAB*, 2025, https://iustlab.org/luana.giangregorio/il-nuovo-reato-di-deepfake-legge-132-2025.
[158] Davide Calcedonio Di Giacinto, "Il nuovo reato di deepfake in Italia: come la legge 132/2025 tutela l'identità digitale," *Studio Legale Di Giacanto*, 2025, https://www.digiacinto.it/2025/10/18/il-nuovo-reato-di-deepfake-in-italia-come-la-legge-132-2025-tutela-lidentita-digitale/.

menggunakan kejahatan tidak langsung (pencemaran nama baik, peniruan identitas, pornografi balas dendam), yang tidak selalu mencakup berbagai manipulasi.[159] Pasal 612-quater yang baru diperkenalkan adalah kemajuan penting untuk menjaga identitas digital dan martabat pribadi di era kecerdasan buatan. Seiring kemajuan teknologi, kerangka hukum harus sering direvisi. Negara Italia, melalui Undang-Undang 132 Tahun 2025, telah telah menempatkan dirinya di garis depan di Eropa dan membuka jalan keterlibatan regulasi lebih lanjut.[160]

Undang-undang ini juga memuat pasal tentang perlindungan data pribadi dalam penggunaan sistem kecerdasan buatan, terdapat dalam Pasal 4 ayat (2) dengan judul "*Princìpi in materia di informazione e di riservatezza dei dati personali*" (prinsip-prinsip mengenai informasi dan kerahasiaan data pribadi). Secara keseluruhan bunyi pasalnya "*L'utilizzo di sistemi di intelligenza artificiale garantisce il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti*...."[161] (penggunaan sistem kecerdasan buatan menjamin pemrosesan data pribadi yang sah, benar, dan transparan serta kesesuaiannya dengan tujuan pengumpulannya).

Istilah sah secara hukum dalam konteks pemrosesan data pribadi berarti setiap aktivitas pengolahan data harus memiliki landasan hukum

[159] Ma, "Italy passes its own law on artificial intelligence: new rules effective October 2025."
[160] Giacinto, "Il nuovo reato di deepfake in Italia: come la legge 132/2025 tutela l'identità digitale."
[161] "Gazzetta Ufficiale," Della Repubblica Italiana, 2025.

yang jelas dan diakui secara resmi.[162] Prinsip ini menuntut bahwa data pribadi tidak dapat diproses tanpa alasan yang sah. Landasan hukum ini menjamin bahwa penerapan data pribadi dalam sistem kecerdasan buatan (*AI*) tidak disalahgunakan, agar tetap mematuhi pedoman yang ditetapkan secara hukum.[163]

Frasa benar atau lebih tepatnya akurat, dalam konteks pemroresan data pribadi, mengharuskan informasi yang digunakan dalam sistem kecerdasan buatan (*AI*) tepat, relevan, dan terkini. Pada dasarnya, ini menyiratkan bahwa data tidak boleh usang, salah, atau menipu, karena ini dapat mengakibatkan hasil pemrosesan kecerdasan buatan (*AI*) yang cacat dan secara signifikan melanggar privasi orang.[164]

Transparansi dalam penanganan data menunjukkan bahwa individu yang datanya sedang diproses harus menerima informasi yang jelas dan dapat dipahami mengenai siapa yang mengelola data mereka, alasan pemrosesan ini, metode yang digunakan, dan hak yang mereka miliki terkait data mereka. Penggunaan kecerdasan buatan (AI) haruslah transparansi. Keterbukaan semacam ini merupakan bagian penting dari hak pemberitahuan dalam undang-undang perlindungan data, yang mencegah terjadinya pengambilan data rahasia atau pemrosesan tanpa

[162] Eyup Kun, "Searching for the Appropriate Legal Basis for Personal Data Processing for Cybersecurity Purposes under the NIS 2 Directive: Legal Obligation and/or Legitimate Interest?," *Computer Law & Security Review* 56 (April 2025): 106, https://doi.org/10.1016/j.clsr.2024.106098.
[163] Philipp Hacker, "A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act," *Law, Innovation and Technology* 13, no. 2 (2021): 258–59, https://doi.org/10.1080/17579961.2021.1977219.
[164] Pablo Trigo Kramcsák, "Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?," *Computer Law & Security Review* 48 (April 2023): 2, https://doi.org/10.1016/j.clsr.2022.105765.

persetujuan.[165] Tidak adanya transparansi dan pembatasan tujuan, penanganan data pribadi dapat dilihat sebagai pelanggaran hak privasi individu.

Undang-undang ini menekankan pentingnya keamanan siber untuk pengmbangan kecerdasan buatan, dengan menugaskan Badan Keamanan Siber Nasional (ACN) tanggung jawab untuk mendorong dan membuat program yang dirancang untuk memanfaatkan kecerdasan buatan sebagai alat untuk meningkatkan keamanan siber nasional. Regulasi undang-undang ini menetapkan kerangka tata kelola yang terstruktur. Kantor Perdana Menteri harus mengembangkan strategi nasional untuk kecerdasan buatan, yang akan disetujui setiap dua tahun sekali oleh Komite Antar Kementerian untuk Transisi Digital (CITD) dan tunduk pada tinjauan tahunan oleh Parlemen, dengan tujuan untuk mengoordinasikan kebijakan publik tentang kecerdasan buatan sekaligus mempromosikan inovasi teknologi sesuai dengan hak-hak fundamental.

Badan Digital Italia (AgID) ditunjuk sebagai badan yang bertanggung jawab untuk mendorong inovasi dan mengembangkan kecerdasan buatan, dengan tanggung jawab mengenai pemberitahuan, evaluasi, akreditasi, dan pengawasan organisasi yang bertanggung jawab untuk memastikan kepatuhan. Badan Keamanan Siber Nasional

[165] Heike Felzmann dkk., "Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns," *Big Data & Society* 6, no. 1 (2019): 2–3, https://doi.org/10.1177/2053951719860542.

(ACN) ditunjuk sebagai otoritas pengawas. Peran spesifik Bank Sentral Italia, CONSOB, dan IVASS untuk area pengawasan pasar masing-masing.[166]

Tabel 3.3

Tabel Analisis Substansi dan Struktur Pengaturan *AI Deepfake* dalam Undang-Undang No. 132 Tahun 2025 (Italia)

No	Substansi	Struktur Lembaga
1.	Undang-Undang No. 132 Tahun 2025 mengatur *AI* secara umum, namun secara eksplisit mencakup *AI* generatif (Pasal 2 dan 3)	Badan Digital Italia (AgID) berperan dalam pemberitahuan, evaluasi, akreditasi, dan pemantauan kepatuhan entitas verifikator *AI*, kemudian Badan Keamanan Siber Nasional (ACN) berwenang melakukan pengawasan terhadap sistem *AI*, termasuk inspeksi dan penjatuhan sanksi, ditunjuk sebagai Otoritas Nasional untuk Kecerdasan Buatan (*AI*) (Bab III Pasal 20 Otoritas Nasional untuk Kecerdasan Buatan)
2.	Kriminalisasi *deepfake* muncul melalui larangan penyebaran konten visual, audio, atau audiovisual hasil manipulasi AI yang menyesatkan dan tanpa persetujuan Diatur dalam Pasal 612-quater (hasil amandemen)	Penegakan sektoral otoritas keuangan yaitu, Bank Sentral Italia, Komisi Nasional untuk Perusahaan dan Bursa Efek (CONSOB) dan Institut Pengawasan Asuransi (IVASS)

[166] Aurora Agostini dkk., "The Law of September 23, 2025, No. 132 on Artificial Intelligence: Principles, Obligations, and Opportunities," *Lexia*, 2025, https://www.lexia.it/es/2025/10/01/law-23-september-artificial-intelligence/.

	mengatur penyebaran ilegal konten yang dihasilkan atau diubah dengan sistem AI	(Bab III Pasal 20 Otoritas Nasional untuk Kecerdasan Buatan)
3.	Sanksi pidana penjara satu hingga lima tahun bagi pelaku penyediaan, publikasi, atau penyebaran konten yang dihasilkan atau diubah dengan sistem AI (Bab V Ketentuan Pidana Pasal 612 quarter)	Dibentuk Komite Koordinasi untuk kegiatan pembuatan kebijakan pada lembaga, organisasi, dan yayasan yang beroperasi di bidang inovasi digital dan kecerdasan buatan. Komite ini diketuai oleh Perdana Menteri atau otoritas politik yang didelegasikan. (Bab III Pasal 19 ayat (5))
4.	Pemberatan pidana dua hingga tujuh tahun jika *AI* digunakan untuk menyebarkan informasi palsu, penipuan atau tipu daya kejahatan keuangan yang berpotensi nyata mengubah harga instrumen keuangan atau merusak kepercayaan publik terhadap stabilitas bank. (Pasal 2637 KUHPer tentang Pelanggaran Pasar Saham)	
5.	Hukuman penjara dua hingga tujuh tahun dan denda €25.000 hingga €6.000.000, jika menyebarkan informasi palsu atau melakukan penipuan dengan tujuan mengubah harga instrumen keuangan secara signifikan. (Pasal 185 tentang Manipulasi Pasar)	

Undang-undang No. 132 tahun 2025 di Italia membahas *deepfake* dengan memasukkannya ke dalam kerangka hukum *AI* generatif dan peraturan pidana yang telah ditetapkan sebelumnya. *Deepfake* dianggap sebagai tindakan berbahaya jika menipu, melanggar persetujuan, menyebabkan kerugian pada orang, atau mengganggu stabilitas keuangan, yang mengarah pada konsekuensi hukum yang signifikan dan hukuman berat.[167]

Pengawasan dikelola melalui kerangka kelembagaan yang terorganisir dengan baik. AgID dan ACN berfungsi sebagai badan utama untuk *AI*, didukung oleh otoritas tertentu seperti Bank Sentral Italia, CONSOB, dan IVASS, bersama dengan Komite Koordinasi Nasional.[168] Struktur ini mencerminkan strategi yang kuat dan terfokus untuk menjaga kepentingan publik dan memastikan stabilitas sistem.

Italia dan Indonesia menempuh jalur yang berbeda dalam mengatur fenomena *deepfake*. Italia telah secara tegas memasukkan *deepfake* ke dalam kerangka hukum kecerdasan buatan generatif sekaligus hukum pidana, sehingga posisinya jelas sebagai objek pengaturan dan pengawasan.[169] Sebaliknya, Indonesia hingga kini belum memiliki pengaturan khusus yang secara eksplisit menyebut *deepfake*.

[167] Nicola Sandon dkk., "Italy Leads the Way: The First National Law on Artificial Intelligence Is Approved," *RODL*, 2025, https://www.roedl.it/en-gb/it/insights/pages/legal-newsletter/9-2025/italy-leads-way-first-national-law-artificial-intelligence-approved.aspx.
[168] Margherita Banfi dkk., "Law No. 132 of 23 September 2025: Italy's Leadership in National AI Regulation," *JDSUPRA*, 2025, https://www.jdsupra.com/legalnews/law-no-132-of-23-september-2025-italy-s-3662716/.
[169] Angela Giuffrida, "Italy First in EU to Pass Comprehensive Law Regulating Use of AI," *The Guardian*, 2025, https://www.theguardian.com/world/2025/sep/18/italy-first-in-eu-to-pass-comprehensive-law-regulating-ai.

Penanganannya masih dilakukan secara tidak langsung melalui berbagai aturan yang tersebar, seperti ketentuan tentang penyebaran informasi palsu, pencemaran nama baik, pornografi, penipuan, serta pelanggaran data pribadi.[170]

Kondisi tersebut menunjukkan adanya jarak yang cukup lebar baik dari sisi norma maupun kelembagaan. Italia memilih pendekatan yang lebih sistematis dan bersifat pencegahan, dengan menilai *deepfake* sebagai bagian dari risiko teknologi *AI* yang perlu diatur sejak awal. Sementara itu, Indonesia masih bertumpu pada pendekatan penindakan setelah peristiwa terjadi, dengan menafsirkan dan memperluas pasal-pasal hukum yang sudah ada untuk menjerat pelaku *deepfake*. Pendekatan ini membuat perlindungan hukum di Indonesia cenderung kurang terstruktur dibandingkan dengan model yang diterapkan di Italia.

Perbedaan pendekatan tersebut berdampak langsung pada perkembangan teknologi *deepfake* yang semakin berbahaya.

[170] Muhammad Afif, "Tindak Pidana Deepfake Pornography di Indonesia: Analisis Yuridis terhadap Kekosongan Norma dalam KUHP dan UU ITE," *Jurnal Ilmiah Multidisiplin* vol 3, no. 2 (2025): 28, https://doi.org/10.62017/merdeka.v3i2.6133.

3. *Legal Vacuum* dalam Pengaturan *Deepfake* di Indonesia

Untuk melihat secara jelas perbedaan pengaturan antara Indonesia dan Italia, perlu dilakukan pemetaan terhadap aspek-aspek pokok yang menjadi titik tekan masing-masing negara. Perbandingan ini meliputi bagaimana definisi dirumuskan, bentuk-bentuk penyalahgunaan yang diakomodasi, jenis sanksi yang diterapkan, serta mekanisme dan kelembagaan pengawasannya dalam konteks kecerdasan buatan dan *deepfake*. Penyusunan dalam bentuk tabel dipilih agar perbedaan karakter dan pendekatan regulasi kedua negara dapat dipahami secara runtut dan menyeluruh.

Tabel 4.3

Perbandingan Pengaturan *Deepfake* di Indonesia dan Italia

No	Substansi	Indonesia	Italia	Keterangan
1.	Definisi *AI* (*deepfake*)	Tidak terdapat definisi khusus tentang *deepfake* atau *AI*	Pasal 2 *Deepfake* diposisikan sebagai bagian dari *AI* generatif dengan definisi dan ruang lingkup yang jelas	Indonesia saat ini pengaturan *deepfake* belum dirumuskan secara tegas dan eksplisit sedangkan italia objek pengaturannya dirumuskan secara jelas
2.	Penyalahgunaan *AI* (*deepfake*)	Bergantung pada interpretasi pasal dan dikaitkan melalui norma umum, seperti pencemaran nama baik, penipuan	Pasal 612-quarter Mengatur penyebaran ilegal konten yang dihasilkan atau dimodifikasi (gambar, video atau suara) dengan sistem kecerdasan buatan	Pengaturan di Indonesia penanganan terhadap *deepfake* baru dilakukan setelah dampaknya muncul dan masih bergantung pada ketentuan yang tersebar di berbagai peraturan perundang-undangan, sedangkan Italia

				mengatur *deepfake* secara tegas sejak awal, termasuk melalui kriminalisasi langsung terhadap perbuatan tersebut.
3.	Sanksi	Undang-Undang No. 27 Tahun 2022 tentang PDP, Pasal 67 dan 68 **Pasal 67:** Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan mililoeya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). (2) Setiap Orang yang dengan sengaja dan melawan hukum mengunglapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak	Bab V Ketentuan Pidana Pasal 26	Indonesia, pengenaan sanksi terhadap perbuatan *deepfake* keberlakuannya bergantung pada terpenuhinya unsur tindak pidana lain yang diatur dalam peraturan perundang-undangan. Italia sanksi diatur secara langsung dan berdiri sendiri, sehingga tidak memerlukan pembuktian unsur tambahan

		Rp4.000.000.000,00 (empat miliar rupiah). (3) Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.00O.OOO.000,00 (lima miliar rupiah). **Pasal 68:** Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntrrngkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 .tipidana dengan pidana penjara paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.0OO. 000.000,00 (enam miliar rupiah). **Undang-Undang No. 1 Tahun 2024 tentang ITE, Pasal 45 sampai 45B** **Pasal 45:** hak menyiarkan, mempertunjukkan,		

		mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rpl.000.000.000,00 (satu miliar rupiah). Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan,dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyakRp 10.000.000.000,00 (sepuluh miliar rupiah). Setiap Orang yang dengan sengaja menyerang		

		kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya ha1 tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik sebagaimana dimaksud dalam Pasal 27A dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/ atau denda paling banyak Rp4O0.000.000,00 (empat ratus juta rupiah). Dalam hal perbuatan sebagaimana dimaksud pada ayat (41 tidak dapat dibuktikan kebenarannya dan bertentangan dengan apa yang diketahui padahal telah diberi kesempatan untuk membuktikannya, dipidana karena fitnah dengan pidana penjara paling lama 4 (empat) tahun dan/ atau denda paling banyak Rp750.000.00O,00 (tujuh ratus lima puluh juta rupiah). **Pasal 45A**		

		Setiap Orang yang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.0O0.0O0.000,00 (satu miliar rupiah). Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut, mengajak, atau orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama,		

		kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas frsik sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.0OO.0O0.000,0O (satu miliar rupiah). Setiap Orang yang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat sebagaimana dimaksud dalam Pasal 28 ayat (3) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.O0O.0O0,00 (satu miliar rupiah). **Pasal 45B** Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban		

		yang berisi ancaman kekerasan dan/ atau menakutnakuti sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau denda paling banyak Rp750.000.000,00 (tqjuh ratus lima puluh juta rupiah).		
4.	Lembaga pengawasan terkait *AI* atau *deepfake*	Tidak ada lembaga khusus untuk *AI* atau *deepfake*	Pasal 20 Terdapat struktur pengawasan *AI* yang terkoordinasi	Ketiadaan lembaga khusus yang menangani kecerdasan artifisial di Indonesia berdampak pada terpecahnya kewenangan antarinstansi, sedangkan Italia telah membangun tata kelola kecerdasan buatan secara terlembaga

Berdasarkan tabel tersebut, dapat dilihat bahwa perbedaan pendekatan regulasi antara Indonesia dan Italia tidak sekadar terletak pada aspek teknis pengaturannya, melainkan juga menunjukkan perbedaan cara pandang dalam menempatkan *deepfake* sebagai objek hukum. Perbedaan paradigma ini penting untuk dicermati, karena memengaruhi arah kebijakan dan model pengaturan yang diterapkan masing-masing negara. Melalui perbandingan tersebut, dapat dianalisis lebih jauh bagaimana kekosongan hukum (*legal vacuum*) di Indonesia

berdampak pada lemahnya efektivitas penegakan hukum serta belum optimalnya perlindungan masyarakat di ruang digital.

Pertama, dari aspek definisi, Indonesia belum memiliki definisi khusus mengenai *deepfake* maupun kecerdasan buatan dalam peraturan perundang-undangan yang berlaku. Tidak adanya definisi ini menyebabkan *deepfake* tidak diposisikan sebagai objek hukum yang berdiri sendiri, melainkan hanya dapat dipahami secara implisit melalui norma umum dalam Undang-Undang ITE dan Undang-Undang Pelindungan Data Pribadi.[171] Sebaliknya, Italia secara tegas menempatkan *deepfake* sebagai bagian dari *AI* generatif dalam kerangka Undang-Undang Kecerdasan Buatan nasional yang terintegrasi dengan EU AI Act, sehingga ruang lingkup *deepfake* memiliki dasar pengaturan yang jelas.[172]

Kedua, dalam hal penyalahgunaan *deepfake* Indonesia masih menggunakan pasal umum seperti pencemaran nama baik, penipuan dan hoaks, karena belum ada aturan khusus yang mengatur soal *deepfake*.[173] Italia, sebaliknya telah mengkriminalisasi penyebaran ilegal konten hasil manipulasi *AI* melalui Pasal 612-quarter yang secara jelas sifat perbuatan *deepfake*.[174]

---

[171] Firdaus dan Puspita, "Peran Hukum Dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital," 6–7.
[172] Jacobacci Avvocati, "AI and Deepfakes: EU and Italian Regulations," *Jacobacci Law*, 2025, https://www.jacobacci-law.com/news-and-publications/ai-and-deepfakes-eu-and-italian-regulations.
[173] Silvia Maharani Iskandar Putri dkk., "Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum," *Jurnal Hukum Legalita* 6, no. 2 (2024): 84, https://doi.org/10.47637/legalita.v6i2.1453.
[174] "New Cybercrimes."

Ketiga, dari sisi sanksi Indonesia sebenarnya sudah memiliki ketentuan pidana dan administratif melalui Undang-Undang PDP dan Undang-Undang ITE. Masalahnya, ketentuan tersebut tidak dibuat khusus untuk menangani kasus *deepfake*, melainkan hanya menargetkan pelanggaran data pribadi atau penyalahgunaan sistem dan informasi elektronik secara umum.[175] Italia telah mengesahkan undang-undang tentang kecerdasan buatan yang juga meliputi sanksi pidana terhadap penggunaan atau menyebarkan konten yang berbahaya seperti *deepfake*.[176]

Keempat, dari aspek kelembagaan Indonesia belum memiliki lembaga pengawasan khusus yang berwenang untuk menangani *AI* termasuk *deepfake*. Pengawasan ditangani oleh lembaga yang sudah ada, misal Kementerian Komunikasi dan Digital (Komdigi) dan Polri atau Bareskim yang dimana tidak memiliki kewenangan pengawasan teknisi langsung terhadap AI, sedangkan Italia telah memiliki lembaga yang secara khusus mengawasi AI yaitu Badan Digital Italia (AgID) dan Badan Keamanan Siber Nasional (ACN) yang ditetapkan sebagai otoritas pengatur utama untuk memastikan kepatuhan dan pengawasan teknis terhadap sistem *AI*.[177]

[175] Arvitto, "Implikasi Hukum Deepfake," 77 dan 80.
[176] Laura Ercoli, "New Italian Law on Artificial Intelligence Effective as of 10 October 2025," *SIB*, 2025, https://www.sib.it/en/flash-news/new-italian-law-on-ai-takes-effect-on-10-october-2025/.
[177] Aiman Kanwal, "Italy's AI Law: A Comprehensive Guide to Law No. 132/2025," *Securiti*, 2025, https://securiti.ai/italy-ai-law-guide/.

Penggunaan teknologi *deepfake* menimbulkan berbagai risiko hukum dan sosial yang tidak selalu berkaitan secara langsung dengan pencemaran nama baik, pelanggaran kesusilaan, ataupun tindak pidana penipuan. Salah satu persoalan utama terletak pada tidak adanya persetujuan individu dalam pemanfaatan data pribadi, khususnya data biometrik seperti wajah dan suara, yang kerap digunakan tanpa sepengetahuan maupun izin dari pemilik data.

Praktik tersebut berpotensi melanggar prinsip perlindungan data pribadi serta hak atas privasi, mengingat teknologi *deepfake* mampu mereplikasi identitas seseorang secara sangat menyerupai kondisi nyata. Selain itu, meskipun tidak selalu ditujukan untuk kepentingan kriminal, penggunaan *deepfake* tetap dapat menimbulkan keraguan publik terhadap keaslian informasi yang beredar dan menciptakan situasi informasi yang menyesatkan. Kondisi ini berdampak signifikan terhadap tingkat kepercayaan masyarakat terhadap informasi digital, karena semakin sulit bagi publik untuk membedakan antara konten yang autentik dan konten hasil manipulasi kecerdasan artifisial.

C. Urgensitas Ratifikasi Konvensi Budapest di Indonesia Perspektif *Maqashid Syariah*

Maqaṣid al-Syariah adalah secara terminologis dan konseptual dalam *usul al-fiqh* menekankan tujuan dan alasan yang ingin dipenuhi oleh hukum Islam *(Syariah)* sebagai kerangka komprehensif pedoman normatif, bukan hanya berfokus pada kata-kata tekstual hukum. Secara bahasa,

maqaṣhid adalah jamak dari *maqsud*, yang diterjemahkan menjadi niat, tujuan, atau sasaran, sedangkan *syariah* menandakan jalan menuju sumber air (hidup), yang secara metaforis dipahami sebagai jalan atau kerangka hukum yang berfungsi sebagai panduan bagi keberadaan manusia baik di kehidupan ini maupun di akhirat.[178]

Para ulama mendefinisikan *maqashid syariah* (tujuan syariah) sebagai sarana untuk mencapai kemaslahatan.[179] Penting untuk memahami bahwa *maqashid* bukan hanya kumpulan tujuan. Ini mewakili pola pikir yang memprioritaskan maslahat (kebaikan dan kemanfaatan) sebagai pokok dari syariah. Menurut al-Ghazali, hukum Islam harus berfungsi sebagai alat untuk menumbuhkan kemaslahatan dan mencegah kerusakan.[180]

Menurut Imam al-Ghazali, *Maqashid Syariah* adalah maslahah. Sementara itu, maslahah diartikan sebagai:[181]

يحفظ أن وهو خمسة الخلق من الشرع ومقصود ،الشرع مقصود على محافظة

هذه حفظه يتضمن ما فكل ومالهم ونسلهم وعقلهم ونفسهم دينهم على هم

ودفعها مفسدة فهو الأصول هذه يفوت ما وكل مصلحة فهو الخمسة الأصول

مصلحة

[178] Husain, "Teori Maqashid Syari'ah," *Sulesana Jurnal Wawasan Keislaman* vol 13, no. 1 (2020): 2, https://doi.org/10.24252/sulesana.v13i1.9946.
[179] Abdussalam dan Abdullah Shodiq, "Maqashid As-Syariah Perspektif Imam Al-Ghazali; Studi Literasi Maslahah Mursalah," *Moderasi : Journal of Islamic Studies* vol 2, no. 2 (2022): 141.
[180] Yohanes Rokade, "Maqashid Al-Syariah Menurut Imam Al-Ghazali: Kajian Filosofis Dan Relevansi Hukum Islam Kontemporer," *Jurnal Edukasi dan Literasi Pendidikan* vol 6, no. 3 (2025): 71.
[181] Khairil Anwar Al Jufri dkk., "Maqasid Syariah Menurut Imam Al-Ghazali Dan Aplikasinya Dalam Penyusunan Undang-Undang Islam Di Indonesia: Maqasid Syariah According To Imam Al-Ghazali And Its Application In The Compilation Of Islamic Law In Indonesia," *Malaysian Journal of Syariah and Law* 9, no. 2 (2021): 78, https://doi.org/10.33102/mjsl.vol9no2.315.

Artinya "Menjaga maksud atau tujuan syarat. Terdapat lima tujuan syarat bagi makhluk, iaitu menjaga agama, jiwa, akal, keturunan dan harta mereka. Setiap perkara yang bermaksud untuk menjaga kelima-lima hal ini, merupakan maslahah, dan setiap perkara yang mampu memusnahkannya, adalah mafsadah, dan menghindari terjadinya mafsadah pula, juga merupakan maslahah"

Imam al-Ghazali mengkategorikan tingkatan *maqashid syariah* menjadi tiga tingkatan yang berbeda yaitu, *daruriyah* (kebutuhan primer), *al-hajjiyat* (kebutuhan sekunder), dan *tahsiniyat* (kebutuhan tersier). Menurut al-Ghazali, tujuan syariah, yang mencakup lima elemen *(al-usul al-Khamsah)* adalah untuk melindungi agama, jiwa, akal, keturunan, dan akal. Oleh karena itu, apa pun yang melindungi kelima aspek ini disebut sebagai maslahat, sedangkan apa pun yang merusaknya disebut mafsadat. Al-Ghazali mengkategorikan kelima hal ini sebagai tingkatan *daruriyah*.[182]

Lingkup disiplin *ushul al-fiqh*, *maqaṣid* menempati peran penting sebagai kerangka panduan untuk memahami menyeluruh tentang hukum syariah, yang tidak hanya memeriksa lafaz (teks) secara terpisah tetapi juga berusaha memahami tujuan mendasar yang diabadikan dalam ketentuan hukum, serta cara berinteraksi dengan prinsip-prinsip *maslahah* (kepentingan masyarakat) dan pencegahan *mafsadah* (bahaya). Kajian kontemporer, *maqaṣid* dianggap bukan sebagai sumber hukum independen

[182] Aris Nur Mu'alim, "Potret Maqasid Syariah Persepektif Abu Hamid Muhammad Bin Muhammad Al-Ghazali At-Thusi As-Syafi'i," *Al-Mawarid: Jurnal Syari`ah & Hukum* vol 4, no. 2 (2022): 117.

yang mirip dengan Al-Qur'an dan Sunnah, melainkan sebagai kerangka evaluatif yang mengarahkan semua tahap ijtihad dan penerapan hukum, termasuk qiyas, istihsan, dan maslaha mursalah, dengan demikian berfungsi sebagai instrumen interpretatif dinamis dalam mengatasi kebutuhan zaman sekarang.[183]

Perkembangan teknologi informasi di era digital telah menyebabkan laju inovasi yang cepat, tetapi juga telah memperkenalkan bahaya baru dalam bentuk kejahatan digital yang lebih rumit. Teknologi *deepfake* yang menggunakan kecerdasan buatan *(AI)* menghasilkan konten digital yang realistis dan menipu yang dapat disalahgunakan untuk penipuan, fitnah, pelecehan seksual online, pencurian identitas, dan pengaruh politik melalui informasi palsu.[184]

Konvensi Budapest tentang Kejahatan Siber dalam konteks global berfungsi sebagai alat hukum yang ditetapkan untuk mengatasi kejahatan digital lintas negara, yang mencakup menciptakan standar kriminal untuk pelanggaran yang dilakukan melalui sistem komputer, memfasilisitasi kerjasama internasional dan menyelaraskan hukum nasional di antara negara-negara yang terlibat.[185] Konvensi ini meskipun dibuat pada tahun 2001, terus menjadi alat yang paling signifikan dan berpengaruh dalam

[183] Muhammad Nazir Alias dkk., "The Position of Maqasid al-Shariahwithin Islamic Legal Sources:A Comprehensive Analysis," *Samarah: Jurnal Hukum Keluarga dan Hukum Islam* vol 9, no. 2 (2025): 939, https://doi.org/10.22373/q4byre51.
[184] Federal Bureau of Investigation, "Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes," *Public Service Announcement*, 2025, https://www.ic3.gov/PSA/2023/psa230605.
[185] Council of Europe, "Action against Cybercrime."

memerangi kejahatan dunia maya karena sikapnya yang tidak bias terhadap teknologi dan cakupannya yang luas mencakup berbagai jenis kejahatan digital.

Berdasarkan *maqaṣid* yang ditetapkan oleh Imam al-Ghazali, yang menyoroti lima kebutuhan esensial (*al-Daruriya*t: agama, jiwa, akal, keturunan, dan harta),[186] upaya pemerintah untuk mendukung perjanjian internasional mengenai kejahatan dunia maya seperti Konvensi Budapest sangat dibenarkan.

1. Ancaman terhadap *ḥifẓ al-din* (agama), penyalahgunaan teknologi *deepfake* dapat menyebabkan penciptaan konten yang salah menggambarkan atau menyinggung simbol agama, tokoh, atau komunitas tertentu, yang berpotensi menghasut konflik dan perpecahan sosial.[187] Materi penipuan semacam ini menimbulkan risiko bagi tatanan psikologis dan moral masyarakat (yang penting untuk menegakkan prinsip-prinsip agama dan etika) dan dapat memicu konflik yang berakar pada agama. Mengatasi masalah ini adalah bagian dari kewajiban hukum untuk melindungi prinsip-prinsip syariah untuk mencegahnya perselisihan sosial.
2. Ancaman terhadap *ḥifẓ al-nafs* (jiwa), *deepfake* sering disalahgunakan untuk mengeksploitasi individu karena alasan menipu, seperti pencurian

[186] Redaksi, "Analisis Maqashid Syari'ah Perspektif Imam Al-Ghazali dan Imam Al-Syatibi," *majelistabligh.id*, 2024, https://majelistabligh.id/analisis-maqashid-syariah-perspektif-imam-al-ghazali-dan-imam-al-syatibi/3/.
[187] Joyzy Pius Egunjobi, "The Misuse of AI-Generated Content in Academic and Religious Settings," *International Journal of Research and Scientific Innovation* XII, no. XV (2025): 872, https://doi.org/10.51244/IJRSI.2025.121500077P.

identitas dan mengubah suara atau penampilan korban, yang secara signifikan mempengaruhi kesejahteraan mental dan stabilitas emosional mereka. Dampaknya melampaui kerugian finansial, menyebabkan tekanan psikologis yang mendalam.[188]

Oleh karena itu, dari sudut pandang *maqaṣid*, undang-undang harus menjaga terhadap ancaman terhadap kehidupan dan rasa aman seseorang. Mratifikasi konvensi budapest akan meningkatkan kerangka hukum dalam mempertahankan standar kriminal internasional yang kompatibel dan menawarkan mekanisme penegakan yang lebih kuat, termasuk berbagi bukti dan kerjasama internasional, memastikan bahwa negara-negara tidak berdiri sendiri ketika menangani kasus-kasus yang sering melintasi batas hukum.

3. Ancaman terhadap *ḥifẓ al-ʿaql* (akal), perlindungan akal melibatkan pencegahan unsur-unsur yang mengaburkan kejelasan dan objektivitas data. *Deepfake* yang menyebarkan misinformasi dan disinformation mengganggu proses rasional dalam pengambilan keputusan publik, berpotensi membahayakan hasil demokrasi dan mengikis kepercayaan pada informasi yang kredibel.[189]

   Situasi ini dapat menyebabkan meningkatnya ketegangan sosial, perpecahan masyarakat, dan efek buruk pada kesejahteraan mental bersama. Ratifikasi instrumen internasional seperti Konvensi Budapest

[188] Ali dkk., "Deepfakes and Victimology."
[189] Alexander Diel dkk., "The Harm of Deepfakes a Scoping Review of Deepfakes' Negative Efects on Human Mind and Behavior," *AI & Society*, 2025, 2, https://doi.org/10.51244/IJRSI.2025.121500077P.

akan membantu Indonesia dalam membangun kerangka hukum yang lebih kuat untuk memerangi misinformasi digital dan melindungi ruang publik digital dari distorsi yang mengancam integritas kolektif masyarakat.

4. Ancaman terhadap *ḥifẓ al-nasl* (keturunan), penyalahgunaan *deepfake* dalam pornografi digital, terutama bila dilakukan tanpa persetujuan, menimbulkan risiko bagi martabat dan reputasi individu termasuk anak di bawah umur dan dapat mengganggu dinamika keluarga dan kestabilan sosial.[190] Menjaga anak-anak akan melindungi generasi saat ini dan masa depan dari tindakan yang melemahkan moral dan ikatan keluarga. Konvensi Budapest menawarkan kerangka kerjasama untuk menargetkan pelanggar transnasional dan meningkatkan kriminalisasi konten tersebut.
5. Ancaman terhadap *ḥifẓ al-māl* (harta), selain dampak non materi *deepfake* juga digunakan untuk penipuan keuangan atau pencurian identitas, yang menyebabkan kerugian ekonomi yang signifikan bagi individu dan perusahaan atau lembaga, seperti bank dan berbagai sektor swasta.[191] Jenis kerugian ini menimbulkan risiko bagi *hifal-mal* karena mengganggu stabilitas keuangan pribadi dan perusahaan dan mengurangi kepercayaan publik dalam transaksi online. Kerangka hukum internasional yang kuat, seperti Konvensi Budapest,

[190] Jürgen Stock, "Beyond Illusions Unmasking The Threat Of Synthetic Media For Law Enforcement," Interpol, 2024, 24.
[191] Edi Saputra, "Bank Digital Waspadai Penyalahgunaan Teknologi "Deepfake"."

memberikan akses ke metode kerjasama yang efisien untuk penyelidikan dan penuntutan lintas negara, sehingga meningkatkan perlindungan harta.

Perspektif *maqashid syariah* menunjukkan bahwa masalah *deepfake* melampaui sekadar teknologi, ini pada dasarnya tentang menjaga kemaslahatan masyarakat dan menghindari bahaya (mafsadah) untuk lima tujuan penting: agama, jiwa, kecerdasan, keturunan dan harta. Analisis terhadap kelemahan Indonesia menunjukkan bahwa sistem hukum nasional yang ada tidak memiliki langkah-langkah yang memadai untuk memastikan *hifz al-nafs* (perlindungan jiwa), dan *hifz al-mal* (harta) terhadap kegiatan kriminal transnasional, terdesentralisasi.Fakta bahwa sebagian besar konten *deepfake* di Indonesia merusak martabat perempuan, digunakan untuk penipuan finansial, mempengaruhi persepsi publik, dan dapat membahayakan stabilitas sosial dan politik, menandakan adanya kegagalan.[192]

Secara keseluruhan, dari sudut pandang *Maqashid Syariah*, urgensi ratifikasi Konvensi Budapest terletak pada kewajiban negara:

1. Menutup celah kerusakan yang ditimbulkan oleh teknologi deepfake yang tidak dapat lagi dikendalikan oleh perangkat hukum nasional.
2. Menguatkan perlindungan terhadap martabat, keamanan, dan kepentingan masyarakat melalui standar global yang telah terbukti efektif.

[192] Indonesian National Police, "Deepfake Violence Against Women Soars: UNDP Warns of 'Alarming AI Misuse,'" *INP*, 2025, https://inp.polri.go.id/artikel/deepfake-violence-against-women-soars-undp-warns-of-alarming-ai-misuse.

3. Memastikan kemampuan negara untuk bertindak preventif, responsif, dan kooperatif terhadap kejahatan teknologi lintas yurisdiksi.

BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan hasil pembahasan dan analisis yang telah diuraikan, maka penulis memberikan kesimpulan sebagai berikut:

1. Urgensi ratifikasi Konvensi Budapest di Indonesia didasarkan pada teori tanggung jawab negara (*state responsibility*) dan *due diligence*. Teori James Crawford menegaskan bahwa negara bertanggung jawab tidak hanya atas tindakan langsungnya, tetapi juga atas kelalaian dalam mencegah pelanggaran hukum internasional yang terjadi di wilayah yurisdiksinya. Indonesia, yang belum memiliki regulasi spesifik untuk menangani kejahatan *deepfake* lintas batas, berpotensi dianggap lalai dalam memenuhi kewajiban *due diligence*. Ratifikasi Konvensi Budapest akan memperkuat kerangka hukum nasional, meningkatkan kapasitas penegakan hukum siber, serta memfasilitasi kerja sama internasional dalam penanganan bukti elektronik, ekstradisi, dan bantuan hukum timbal balik (*mutual legal assistance*). Dengan demikian, ratifikasi ini merupakan langkah strategis untuk memenuhi tanggung jawab negara dalam melindungi warga negara dan menjaga keamanan siber nasional.
2. Pengaturan *deepfake* di Indonesia masih bersifat terbatas dan tidak menyeluruh, berbeda dengan pendekatan regulasi yang lebih maju di Italia. Indonesia mengandalkan ketentuan umum dalam Undang-

Undang ITE dan Undang-Undang PDP yang tidak secara eksplisit mengatur *deepfake*, sehingga penanganan kasus cenderung responsif dan bergantung pada penafsiran pasal-pasal yang ada. Sementara itu, Italia telah mengadopsi Undang-Undang No. 132 Tahun 2025 yang secara tegas mengkriminalisasi penyebaran konten *deepfake* tanpa persetujuan, dengan sanksi pidana yang jelas serta kerangka kelembagaan yang terkoordinisasi. Perbandingan ini menunjukkan bahwa Indonesia memerlukan regulasi khusus yang mendefinisikan *deepfake*, menetapkan sanksi yang proporsional, dan membentuk lembaga pengawasan yang berwenang menangani teknologi kecerdasan buatan.

3. Urgensi pengaturan pencegahan penyalahgunaan *deepfake* di Indonesia juga didasarkan pada perspektif *Maqashid Syariah* yang menekankan perlindungan lima kebutuhan dasar (*al-dharuriyyat al-khamsah*). Penyalahgunaan *deepfake* dapat mengancam:

    a. *Hifzh al-din* (agama), melalui konten yang menyesatkan atau memecah belah umat;
    b. *Hifzh al-nafs* (jiwa), dengan menyebabkan trauma psikologis dan gangguan mental;
    c. *Hifzh al-'aql* (akal), melalui disinformasi yang merusak nalar publik;
    d. *Hifzh al-nasl* (keturunan), via konten pornografi non-konsensual yang merusak martabat dan kehormatan keluarga

e. *Hifzh al-mal* (harta), lewat penipuan finansial berbasis rekayasa digital.

Ratifikasi Konvensi Budapest sejalan dengan prinsip *jalb al-maslahah* (mendatangkan kemaslahatan) dan *dar'u al-mafsadah* (menolak kerusakan), karena dapat memperkuat perlindungan terhadap kelima aspek tersebut melalui harmonisasi hukum nasional dengan standar internasional dan peningkatan kapasitas penegakan hukum yang berkeadilan.

B. Saran

Berdasarkan hasil pembahasan dan analisis yang telah diuraikan, maka penulis memberikan saran sebagai berikut:

1. **Kepada Legislator**, disarankan untuk segera mempertimbangkan dan mempercepat proses ratifikasi Konvensi Budapest tentang Kejahatan Siber (*Budapest Convention on Cybercrime*)**.** Ratifikasi ini penting untuk memperkuat kerangka hukum nasional dalam menghadapi kejahatan siber lintas batas, termasuk penyalahgunaan teknologi *deepfake*, serta meningkatkan kapasitas kerja sama internasional dalam penanganan bukti digital dan ekstradisi pelaku dan disarankan untuk menyusun pengaturan yang secara khusus mengatur teknologi *deepfake* dan kecerdasan buatan (*AI*). Pengaturan ini hendaknya mencakup definisi hukum, mekanisme pencegahan, sanksi pidana yang tegas, serta kewajiban transparansi dan akuntabilitas bagi pengembang dan pengguna teknologi AI.

2. **Kepada Lembaga Penegak Hukum,** diharapkan untuk meningkatkan kapasitas teknis dan keahlian di bidang digital forensik serta investigasi kejahatan siber, khususnya terkait deteksi dan pelacakan *deepfake*. Pelatihan berkelanjutan dan kerjasama dengan ahli teknologi informasi diperlukan agar penegakan hukum dapat mengikuti dinamika kejahatan digital yang semakin canggih.
3. **Kepada masyarakat sipil, media, dan platform digital**, diperlukan peran aktif dalam meningkatkan literasi digital serta kesadaran hukum masyarakat terkait bahaya penyalahgunaan teknologi *deepfake*. Upaya ini dapat dilakukan melalui penguatan kampanye edukatif, penerapan mekanisme verifikasi konten, serta optimalisasi pelaporan terhadap konten yang bersifat manipulatif.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Italia. *Undang-Undang Nomor 132 Tahun 2025 tentang Ketentuan dan kewenangan yang didelegasikan kepada Pemerintah terkait kecerdasan buatan.*

Republik Indonesia. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*. Pasal 28F, 28G ayat(1) dan 28I.

Republik Indonesia. *Undang-Undang Nomor Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektonik.*

Republik Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*

Buku

Abdullah Sulaiman. Pengantar Ilmu Hukum. Cetakan kedua. UIN Jakarta bersama Yayasan Pendidikan dan Pengembangan Sumber Daya Manusia, 2020.

Crawford, James. "The International Law Comission's Articles On State Responbility." Cambridge University Press, 2002.

Dixon, Martin, Robert McCorquodale, dan Sarah Williams. "11. State Responsibility." Dalam Cases & Materials on International Law, oleh Martin Dixon, Robert McCorquodale, dan Sarah Williams. Oxford University Press, 2016. https://doi.org/10.1093/he/9780198727644.003.0011.

Jovanovic, Marija. "Positive Obligations as a Means of Establishing State Responsibility for 'Modern Slavery' in Human Rights Law." Dalam State Responsibility for 'Modern Slavery' in Human Rights Law, 1 ed., oleh Marija Jovanovic. Oxford University PressOxford, 2023. https://doi.org/10.1093/oso/9780192867087.003.0005.

Muhaimin. Metode Penelitian Hukum. Cetakan pertama. Mataram University Press, 2020.

Noor Harisudin. Maqashid Syariah: Metode Subtantif Menuju Hukum Keluarga Baru. Cetakan pertama. CV. Literasi Nusantara Abadi, 2022.

Nugroho, Sigit Sapto, Anik Tri Haryani, dan Farkhani. Metodologi Riset Hukum. Cetakan pertama. Oase Pustaka, 2020.

Ramadhan, Muhammad Citra. Buku Ajar - Metode Penelitian Hukum. CV. Kaizen Sarana Edukasi, 2023.

Solikin, Nur. Pengantar Metodologi Penelitian Hukum. Cetakan pertama. CV. Penerbit Qiara Media, 2021.

Sutisna, Neneng Hasanah, Arlinta Prasetian Dewi, dkk. Panorama Maqashid. Media Sains Indonesia, 2021.

Wiwik Sri Widiarty. Metode Penelitian Hukum. Cetakan pertama. Publika Global Media, 2024.

Artikel Jurnal

Abdussalam, dan Abdullah Shodiq. "Maqashid As-Syariah Perspektif Imam Al-Ghazali; Studi Literasi Maslahah Mursalah." Moderasi : Journal of Islamic Studies vol 2, no. 2 (2022): 141.

Afif, Muhammad. "Tindak Pidana Deepfake Pornography di Indonesia: Analisis Yuridis terhadap Kekosongan Norma dalam KUHP dan UU ITE." Jurnal Ilmiah Multidisiplin vol 3, no. 2 (2025): 28. https://doi.org/10.62017/merdeka.v3i2.6133.

Ali, Mahrus, Zico Junius Fernando, Chairul Huda, dan Mahmutarom Mahmutarom. "Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims." Substantive Justice International Journal of Law 8, no. 1 (2025): 3–4. https://doi.org/10.56087/substantivejustice.v8i1.306.

Alias, Muhammad Nazir, Muhammad Najib Abdullah, Mohd Farihal Osman, Nor Faizah Ismail, dan Mohd Sham Kamis. "The Position of Maqasid al-Shariahwithin Islamic Legal Sources:A Comprehensive Analysis." Samarah: Jurnal Hukum Keluarga dan Hukum Islam vol 9, no. 2 (2025): 939. https://doi.org/10.22373/q4byre51.

Apriyanti, Ira. "The Urgency of Establishing Personal Data Protection Act and Financial Technology Act in Digital Era in Order to Protect and Control the

Privacy in Indonesia." Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019), 2020, 345. https://doi.org/10.2991/aebmr.k.200321.045.

Arvitto, Rafi Satrya. "Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP." Jurnal Ilmiah Hukum dan Hak Asasi Manusia 4, no. 2 (2025): 73–82. https://doi.org/10.35912/jihham.v4i2.3937.

Arvitto, Rafi Satrya. Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP (Legal Implications of Deepfake: A Review of the ITE Law and the PDP Law). 4, no. 2 (2025).

Ayu Agung Rasmi Wulan, Ida, dan Ni Luh Gede Astariyani. "Urgensi dalam Meratifikasi Convention On Cybercrime sebagai Pemenuhan HAM di Indonesia." Jurnal Kertha Patrika vol 45 (Agustus 2023). https://doi.org/10.24843/KP.2023.v45.i02.p06.

Basah, Desty Aster Yansen, Andika Wijaya, dan Ivans Januardy. "Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake di Media Sosial." Innovative: Journal Of Social Science Research Vol 5, no. 4 (2025): hal 8-9. https://doi.org/10.31004/innovative.v5i4.20258 .

Butarbutar, Russel. "Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia." International Conference on Law and Governance, 2019.

Chairani, Meirza Aulia, Krista Yitawati, dan Angga Pramodya Pradhana. "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake." Jurnal Rechtens 13, no. 1 (2024): 81–96. https://doi.org/10.56013/rechtens.v13i1.2668.

Chandra, Jansen, Vincent Tanaka, dan Ricky Banke. "Peran Interpol dalam Menangani dan Menanggulangi KejahatanSiber di Indonesia." PESHUM : Jurnal Pendidikan, Sosial dan Humaniora vol 4, no. 3 (2025): 4711.

Chesney, Robert, dan Danielle K. Citron. "Deep Fakes: A Looming Challenge for Priv Es: A Looming Challenge for Privacy, Democr , Democracy, and National Security." Boston University School of Law, 2020.

Diel, Alexander, Tania Lalgi, Finley Sam Mellis, Alexander Teufel, dan Alexander Bäuerle. “The Harm of Deepfakes a Scoping Review of Deepfakes’ Negative Efects on Human Mind and Behavior.” AI & Society, 2025, 2. https://doi.org/10.51244/IJRSI.2025.121500077P.

Doing, Muhammad, Yuko Fitrian, Sy Muhammad Ridho Rizki Maulufi Alkadrie, Muhammad Reza Fahlevi, Aprieyanti, dan Warriyodi. “Legal Challenges In Combating Deepfake Abuse: A Comparative Studyof Ai Regulation In Privacy Protection And Digital Security.” International Conference Restructuring and Transforming Law 2 vol 4, no. 1 (2025): 638.

Egunjobi, Joyzy Pius. “The Misuse of AI-Generated Content in Academic and Religious Settings.” International Journal of Research and Scientific Innovation XII, no. XV (2025): 871–79. https://doi.org/10.51244/IJRSI.2025.121500077P.

Faculty of Law, International Vision University, Abdulmecit Nuredin, Tevfik Can İNan, dan Faculty of Law, International Vision University. “Cyber Warfare And International Criminal Law: State Responsibility For Cyber Attacks.” Congress Proceedings, 24 Oktober 2024, 189–201. https://doi.org/10.55843/ISC2024conf189n.

Fahamsyah, Ermanto, Vicko Taniady, Kania Venisa Rachim, dan Novi Wahyu Riwayanti. “Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention.” De Jure: Jurnal Hukum dan Syar’iah 14, no. 1 (2022): 140–59. https://doi.org/10.18860/j-fsh.v14i1.15731.

Felzmann, Heike, Eduard Fosch Villaronga, Christoph Lutz, dan Aurelia Tamò-Larrieux. “Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns.” Big Data & Society 6, no. 1 (2019): 2–3. https://doi.org/10.1177/2053951719860542.

Firdaus, Hazmin Sulton, dan Lona Puspita. “Peran Hukum Dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital.” UIR Law Review vol 9, no. 1 (2025): 5–6.

Hacker, Philipp. “A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act.” Law, Innovation and Technology 13, no. 2 (2021): 258–59. https://doi.org/10.1080/17579961.2021.1977219.

Haryono, Eko, Siti Suprihatiningsih, Damar Septian, Joko Widodo, Ali Ashar, dan Sariman. “New Paradigm Metode Penelitian Kepustakaan (Library Research) di Perguruan Tinggi.” An-Nur: The Journal of Islamic Studies Vol 14, no. 1 (2024): 3.

Husain. “Teori Maqashid Syari’ah.” Sulesana Jurnal Wawasan Keislaman vol 13, no. 1 (2020): 2. https://doi.org/10.24252/sulesana.v13i1.9946.

Itsna Hidayatul Khusna Sri Pangestuti. “Deepfake, Tantangan Baru Untuk Netizen.” PROMEDIA Vol 5 (2020): 6.

Judijanto, Loso, Andrew Shandy Utama, dan Heri Setiyawan. “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia.” The Easta Journal Law and Human Rights 3, no. 02 (2025): 105–7. https://doi.org/10.58812/eslhr.v3i02.470.

Jufri, Muhammad Ariq Abir, dan Akbar Kurnia Putra. “Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi.” Uti Possidetis: Journal of International Law 2, no. 1 (2021): 31–57. https://doi.org/10.22373/up.v2i1.11093.

Juwana, Hikmahanto. “Hukum Internasional Sebagai Instrumen Politik: Beberapa Pengalaman Indonesia Sebagai Studi Kasus.” Arena Hukum 5, no. 2 (2012): 106–14. https://doi.org/10.21776/ub.arenahukum.2012.00502.4.

Kelman, Mykhailo, dan Rostislav Kelman. “Doctrine approaches to the disclousure of the concept of ‘Legal regulation.’” Visnik Nacional’nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki 10, no. 39 (2023): 13. https://doi.org/10.23939/law2023.39.013.

Kornelius Benuf dan Muhamad Azhar. “Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer.” Jurnal Gema Keadilan Vol 7, no. 1 (2020): 23–24.

Kramcsák, Pablo Trigo. “Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?” Computer Law & Security Review 48 (April 2023): 2. https://doi.org/10.1016/j.clsr.2022.105765.

Kristiyenda, Yoan Shevila, Jasmine Faradila, dan Christina Basanova. “Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang.” ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora 3, no. 2 (2025): 149–64. https://doi.org/10.59246/aladalah.v3i2.1263.

Kun, Eyup. “Searching for the Appropriate Legal Basis for Personal Data Processing for Cybersecurity Purposes under the NIS 2 Directive: Legal Obligation and/or Legitimate Interest?” Computer Law & Security Review 56 (April 2025): 106. https://doi.org/10.1016/j.clsr.2024.106098.

Laksito, Joni, Maulana Fahmi Idris, dan Agus Waryanto. “Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif.” Hakim: Jurnal Ilmu Hukum dan Sosial 2, no. 4 (2024): 774–90. https://doi.org/10.51903/hakim.v2i4.2154.

Laza, Jeremiah Maximillian, dan Rizky Karo Karo. “Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP dan GDPR [Legal Protection of Artificial Intellegence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR].” Lex Prospicit 1, no. 2 (2023): 136. https://doi.org/10.19166/lp.v1i2.7386.

Lipkina, Nadezhda N., dan Dmitry V. Krasikov. “The International Legal Obligation Of Due Diligence In Cyberspace.” 20 Januari 2022, 392–97. https://doi.org/10.15405/epsbs.2022.01.63.

Liu, Ian Yuying. “State Responsibility and Cyberattacks: Defining Due Diligence Obligations 4(2) The Indonesian Journal of International and Comparative Law 191-260.” The Indonesian Journal of International & Comparative Law, 2017, 193.

Mackenzie-Gray Scott, Richard. “Due Diligence as a Secondary Rule of General International Law.” Leiden Journal of International Law 34, no. 2 (2021): 343–72. https://doi.org/10.1017/S0922156521000030.

Mania, Karolina. “Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study.” Trauma, Violence, & Abuse 25, no. 1 (2024): 122. https://doi.org/10.1177/15248380221143772.

Maulia, Savana, dan Sidi Ahyar Wiraguna. “Penyalahgunaan Foto Berbasis AI Dan Tantangan Hukum Berdasarkan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi.” Jurnal Hukum dan Kewarganegaraan vol 12, no. 3 (2025): 3. https://doi.org/10.3783/causa.v12i3.12778.

Mcdonald, Neil. “The Role Of Due Diligence In International Law.” Cambridge University Press for the British Institute of International and Comparative Law, 2020, 1042.

Meliana, Yang. “Urgensi Formulasi Perlindungan Hukum Dan Kepastian Pidana Terhadap Pengaturan Tindak Pidana Deepfake Dalam Sistem Hukum Pidana Nasional The Urgency Of Formulating Legal Protection And Criminal Law Certainty Regarding The Regulation Of Deepfake Crimes Within The Indonesian Criminal Law System.” Rewang Rencang : Jurnal Hukum Lex Generalis vol 6, no. 7 (2025): 2–3.

Misirlis, Nikolaos, dan Harris Bin Munawar. “From Deepfake To Deep-Useful: Risks And Opportunities Through A Systematic Literature Review.” International Conferences e-Society, 2022.

Mu’alim, Aris Nur. “Potret Maqasid Syariah Persepektif Abu Hamid Muhammad Bin Muhammad Al-Ghazali At-Thusi As-Syafi’i.” Al-Mawarid: Jurnal Syari`ah & Hukum vol 4, no. 2 (2022): 117.

Muhshi, Adam. “Pemenuhan Hak atas Informasi Publik sebagai Tanggung Jawab Negara dalam rangka Mewujudkan Good Governance.” Lentera Hukum vol 5, no. 1 (2020): 64. https://doi.org/10.19184/ejlh.v5i1.7284.

Mutmainnah, Anti, Awalia Marwah Suhandi, dan Yusuf Tri Herlambang. “Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang

Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital." UPGRADE : Jurnal Pendidikan Teknologi Informasi 1, no. 2 (2024): 67–72. https://doi.org/10.30812/upgrade.v1i2.3702.

Noerman, Chiquita Thefirstly, dan Aji Lukman Ibrahim. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara." Jurnal Usm Law Review 7, no. 2 (2024): 603–21. https://doi.org/10.26623/julr.v7i2.8995.

Nugraha Isa, Saptha, Rahmayanti, dan Krismanto Manurung. "Criminal Law Policy in Dealing With The Development of Transnational Cyber Crime." International Journal of Sociology and Law Vol 2, no. 2 (2025): 118. https://doi.org/10.62951/ijsl.v2i2.652.

Nurdin, Sri Wahyuni, dan Imam Fadhil Nugraha. "Ancaman Deepfake Dan Disinformasi Berbasis Ai: Implikasi Terhadap Keamanan Siber Dan Stabilitas Nasional Indonesia." JIMR: Journal Of International Multidisciplinary Research vol 4, no. 1 (2025): 74. https://doi.org/10.62668/jimr.v4i01.1551.

Paddeu, Federica, dan Christian J Tams. "Encoding the law of State responsibility with courage and resolve: James Crawford and the 2001 Articles on State Responsibility." Cambridge International Law Journal 11, no. 1 (2022). https://doi.org/10.4337/cilj.2022.01.01.

Papilaya, Billy Diego Arli, Johanis Steny Franco Peilouw, dan Waas Richard Marsilio. "Tanggung Jawab Negara Terhadap Pelanggaran Hak Asasi Manusia Di Belarusia Ditinjau Dari Hukum Internasional." Tatohi Jurnal Ilmu Hukum vol 1, no. 6 (2021): 536–37.

Paryadi. "Maqashid Syariah : Definisi Dan Pendapat Para Ulama." Universitas Islam Negeri Sultan Syarif Kasim Riau Vol 4, no. 2 (2021): 215.

Pertiwi, Tanza Dona, dan Sri Herianingrum. "Menggali Konsep Maqashid Syariah: Perspektif Pemikiran Tokoh Islam." Jurnal Ilmiah Ekonomi Islam Vol 10, no. 1 (2024): 814.

Putri, Kartika Ardina Raesyah, Haris Djoko Saputro, dan Aliesa Amanita. "Legal Liability For Using Artificial Intelligence To Produce Deepfakes Under Personal Data Protection Lawpertanggungjawaban Hukum Atas

Penggunaan Artificial Intelligenceuntuk Deepfakemenurut Uu Perlindungan Data Pribadi." Jurnal Rechswetenschap, 2025, 13–14. https://doi.org/10.36859/rechtswetenschap.v2i2.3962.

Putri, Silvia Maharani Iskandar, Nashwa Salsabila, dan Asmak Ui Hosnah. "Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum." Jurnal Hukum Legalita 6, no. 2 (2024): 83–90. https://doi.org/10.47637/legalita.v6i2.1453.

Rahman, Rofi Aulia, dan Rizaldy Anggriawan. "Deepfake and Election Crimes:Comparative Perspectives from Indonesia,India,Pakistan,and theU.S." Indonesian Comparative Law Review vol 7, no. 2 (2025): 134. https://dx.doi.org/10.18196/iclr.v7i2.26337.

Rezi, Muhamad, Maman Rahman Hakim, dan Suhaimi. "Al-Maqâshid Al-Syarî'ah ; Teori dan Implementasi." Sahaja Journal Sharia And Humanities vol 2, no. 1 (2023): 159.

Risno, Kamarudin, dan Kamlan Dagani. "Pertanggungjawaban Pidana Terhadap Pelaku Deepfake Pornograph." Jurnal Tana Mana vol 6, no. 3 (2025): 186. https://doi.org/10.33648/jtm.v6i3.1320.

Rokade, Yohanes. "Maqashid Al-Syariah Menurut Imam Al-Ghazali: Kajian Filosofis Dan Relevansi Hukum Islam Kontemporer." Jurnal Edukasi dan Literasi Pendidikan vol 6, no. 3 (2025): 71.

Rosidi, Ahamad, M Zainuddin, dan Ismi Arifiana. "Metode Dalam Penelitian Hukum Normatif Dan Sosiologis (Field Research)." Journal Law and Government 2, no. 1 (2024): 46. https://doi.org/10.31764/jlag.v2i1.21606.

Seveney, Madalaine Christella, Demas Brian Wicaksono, dan Irwan Kurniawan Soetijono. "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi." Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum sumpah Pemuda 31, no. 2 (2025): 97–106. https://doi.org/10.46839/disiplin.v31i2.1167.

Shavkat Shukhrat Ugli, Nurilloev. "The Foundations Of State Responsibility In International Law: An In-Depth Analysis Of Key Principles And Norms." European Journal of Contemporary Business Law & Technology: Cyber

Law, Blockchain, and Legal Innovations 1, no. 9 (2024): 100. https://doi.org/10.61796/ejcblt.v1i9.1031.

Zainal Abidin. "Urgensi Maqashid Syariah bagi Kemashlahatan Umat." Jurnal Kajian Keislaman vol 1 (2023): 126.

Laporan dan Dokumen

"Action against Cybercrime." Council of Europe, t.t. Diakses 9 Mei 2025. https://www.coe.int/en/web/cybercrime.

Budapest. "Convention on Cybercrime." European Treaty Series, 2001.

Committee of Ministers. "Council of Europe modernises provisions for mutual assistance in criminal matters." Council of Europe, 2025. https://www.coe.int/en/web/portal/-/council-of-europe-modernises-provisions-for-mutual-assistance-in-criminal-matters.

"Convention on Cybercrime (ETS No. 185) –." Cybercrime Convention Committee (T-CY), 2020. https://rm.coe.int/09000016809f44f0.

Council of Europe. "Action against Cybercrime." Digital Governance. Council of Europe, 2022. https://www.coe.int/en/web/digital-governance/cybercrime.

Crawford, James. "First Report on State Responsibility, by Mr. James Crawford." Legal UN, 1998.

Europol. "Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers." EUROJUST, 2024. https://www.eurojust.europa.eu/sites/default/files/assets/trans-border-access-to-stored-computer-data-under-article-32-of-the-budapest-convention-on-cybercrime-and-extraterritorial-powers-23-01-2024.pdf .

Federal Bureau of Investigation. "Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes." Public Service Announcement, 2025. https://www.ic3.gov/PSA/2023/psa230605.

"Gazzetta Ufficiale." Della Repubblica Italiana, 2025.

Kesavarajah, Abiraam, Hewad Tahiri, Liam Cunningham, Rex Pallath, dan Tao Wu. "Deepfake Technology Unveiled: The Commoditization of AI and Its Impact on Digital Trust." Cornell University, 2025.

Mirsky, Yisroel. “The Creation and Detection of Deepfakes: A Survey.” Georgia Institute of Technology and Ben-Gurion University, 2020.

Nugraha, Yudo Agnastio. “Implementasi Konvensi Budapest (2001) Dalam Penanganan Kejahatan Siber.” Universitas Lampung, 2025.

Pangerapan, Samuel Abrijani. “Naskah Akademik Rancangan Undang-Undang Tentang Perubahan Kedua Atas Undangundang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.” Kementerian Komunikasi dan Informatika, 2021.

Sasongko, Ashwin. “General Remaks The Director General Of Ict Application Ministry Of Communication And Information Technology Republic Of Indonesia 23 - 25 March, 2010, Strasbourg, France.” Conference paper presented pada Octopus Interface Conference, Perancis. 2010.

Soofi, Ahmer Bilal, dan Muhammad Khalid Masud. International Law and Maqasid Al-Shariah. 2024, hal 2-3.

Stock, Jürgen. “Beyond Illusions Unmasking The Threat Of Synthetic Media For Law Enforcement.” Interpol, 2024.

Strasbourg. “Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY.” Council of Europe, 2025. https://www.coe.int/en/web/cybercrime/parties-observers?utm.

Strasbourg. “The Budapest Convention on Cybercrime: Benefits and Impact in Practice.” Cybercrime Convention Committee (T-CY), 2020.

Strasbourg. “The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols.” Council of Europe, 2025. https://www.coe.int/en/web/cybercrime/the-budapest-convention?

Website

Agostini, Aurora, Giovanni Lombardi, Giulietta Minucci, dan Alessandro Carlini. “The Law of September 23, 2025, No. 132 on Artificial Intelligence: Principles, Obligations, and Opportunities.” Lexia, 2025. https://www.lexia.it/es/2025/10/01/law-23-september-artificial-intelligence/.

Andartanto, Jemi. “Apa Itu Deepfake? Kenali Bahaya dan Cara Mendeteksinya.” Dinas Kominfo Kab. Kubu Raya, 2024. https://kominfo.kuburaya.go.id/apa-itu-deepfake-kenali-bahaya-dan-cara-mendeteksinya.

Avvocati, Jacobacci. “AI and Deepfakes: EU and Italian Regulations.” Jacobacci Law, 2025. https://www.jacobacci-law.com/news-and-publications/ai-and-deepfakes-eu-and-italian-regulations.

Banfi, Margherita, Claudio Chiarella, dan Francesca Corbinelli. “Law No. 132 of 23 September 2025: Italy’s Leadership in National AI Regulation.” JDSUPRA, 2025. https://www.jdsupra.com/legalnews/law-no-132-of-23-september-2025-italy-s-3662716/.

Budiarti, Irma. “Apa Itu Deepfake? Ini Bahayanya.” Berita. detiknews.com, 2025. https://www.detik.com/jatim/berita/d-8090720/apa-itu-deepfake-ini-bahayanya.

Edi Saputra, Emanuel. “Bank Digital Waspadai Penyalahgunaan Teknologi ”Deepfake”.” Artikel. kompas.id, 2025. https://www.kompas.id/artikel/bank-digital-waspadai-penyalahgunaan-teknologi-deepfake.

Ercoli, Laura. “New Italian Law on Artificial Intelligence Effective as of 10 October 2025.” SIB, 2025. https://www.sib.it/en/flash-news/new-italian-law-on-ai-takes-effect-on-10-october-2025/.

Faridah, Siti. “Adapun Pengertian Dari Metode Deskriptif Analitis Menurut Sugiono.” Scribd, 2016. https://www.scribd.com/doc/306349047/Adapun-Pengertian-Dari-Metode-Deskriptif-Analitis-Menurut-Sugiono.

Giacinto, Davide Calcedonio Di. “Il nuovo reato di deepfake in Italia: come la legge 132/2025 tutela l’identità digitale.” Studio Legale Di Giacanto, 2025. https://www.digiacinto.it/2025/10/18/il-nuovo-reato-di-deepfake-in-italia-come-la-legge-132-2025-tutela-lidentita-digitale/.

Giangregorio, Luana. “Il nuovo reato di Deepfake (Legge 132/2025).” IUSTLAB, 2025. https://iustlab.org/luana.giangregorio/il-nuovo-reato-di-deepfake-legge-132-2025.

Giuffrida, Angela. “Italy First in EU to Pass Comprehensive Law Regulating Use of AI.” The Guardian, 2025. https://www.theguardian.com/world/2025/sep/18/italy-first-in-eu-to-pass-comprehensive-law-regulating-ai.

H, Misrohatun. “Kominfo Terbitkan Surat Edaran Etika Penggunaan dan Pemanfaatan AI.” IDN TIMES, 2023. https://www.idntimes.com/tech/trend/kominfo-terbitkan-surat-edaran-etika-penggunaan-dan-pemanfaatan-ai-00-h7csw-dpvng4.

Indonesian National Police. “Deepfake Violence Against Women Soars: UNDP Warns of ‘Alarming AI Misuse.’” INP, 2025. https://inp.polri.go.id/artikel/deepfake-violence-against-women-soars-undp-warns-of-alarming-ai-misuse.

Kanwal, Aiman. “Italy’s AI Law: A Comprehensive Guide to Law No. 132/2025.” Securiti, 2025. https://securiti.ai/italy-ai-law-guide/.

Kemp, Simon. “Digital 2025: Indonesia.” wearesocial.com, 2025. https://datareportal.com/reports/digital-2025-indonesia.

Kinza Yasar. “What is deepfake technology?” TechTarget, 2025. https://www.techtarget.com/whatis/definition/deepfake?

Lavagnini, Simona. “Italy Adopted the First National Law on Artificial Intelligence.” AIPPI, 2025. https://www.aippi.org/news/italy-adopted-the-first-national-law-on-artificial-intelligence/.

law notes. “Global Responses to Cybercrime: The Convention on Cybercrime by the Council of Europe.” Regulation of Cyberspace. The Law Institute, 2023. https://thelaw.institute/regulation-of-cyberspace/global-responses-convention-on-cybercrime-council-europe/.

Law Notes. “The Council of Europe’s Cybercrime Convention: A Framework for International Cybersecurity.” The Law Institute, 2023. https://thelaw.institute/regulation-of-cyberspace/council-europe-cybercrime-convention-framework.

Leggat, Helaine. “A New Look at the Budapest Convention on Cybercrime.” ITCL, t.t. Diakses 3 Desember 2025. https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/.

Liz Walter. “Cambridge Dictionary.” Dalam Cambridge Dictionary. Cambridge University Press & Assessment, 2025. Cambridge Dictionary.

Luqman Hakim. “Urgensi Adalah: Pengertian, Jenis, dan Cara Menghadapi.” deepublish, 2024. https://deepublishstore.com/blog/urgensi/.

Ma, Andrew. “Italy passes its own law on artificial intelligence: new rules effective October 2025.” The AI Forum Exploring the legal and social challenges of AI, 2025. https://www.theaiforum.org/news-were-reading/italy-passes-first-national-ai-law.

Maimunah, Siti. “Apa Itu Deepfake?” INCA University, 2025. https://inca.ac.id/deepfake/.

Martin, Elizabeth A. “A Dictionary of Law.” Dalam Oxford Dictionary of Law, 5 ed. Oxford Paperback Reference, 2002.

Muamar, Abul. “Kominfo Terbitkan Surat Edaran terkait Etika Penggunaan AI.” green network, 2024. https://greennetwork.id/gna-knowledge-hub/kominfo-terbitkan-surat-edaran-terkait-etika-penggunaan-ai/.

Patria, Nezar. “Deepfake Jadi Modus Kejahatan Siber Baru, Wamen Nezar Tegaskan Pentingnya Mitigasi Risiko.” KOMDIGI, 2025. https://www.komdigi.go.id/berita/siaran-pers/detail/deepfake-jadi-modus-kejahatan-siber-baru-wamen-nezar-tegaskan-pentingnya-mitigasi-risiko.

Poidevin, Olivia Le. “UN Report Urges Stronger Measures to Detect AI-Driven Deepfakes.” Reuters, 2025. https://www.reuters.com/business/un-report-urges-stronger-measures-detect-ai-driven-deepfakes-2025-07-11/.

Pradianto, Fajar El. “Pemanfaatan Teknologi AI Kudu Perhatikan Etika.” RM.id, 2023. https://rm.id/baca-berita/government-action/203115/se-no92023-terbit-pemanfaatan-teknologi-ai-kudu-perhatikan-etika?

Publications Office. “Convention on cybercrime.” Access to European Union law. EUR-Lex, 2023. https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html

Pujiati. “Peraturan yang Mengatur Tentang Artificial Intelligence.” deepublish, 2025. https://penerbitdeepublish.com/peraturan-yang-mengatur-tentang-artificial-intelligence/.

Putri, Aliya R. “Bahaya Laten Deepfake: Wajah Diganti, Realitas Dipalsukan.” kumparan.com, 2025. https://kumparan.com/kumparannews/bahaya-laten-deepfake-wajah-diganti-realitas-dipalsukan-24WchNJRUkJ/.

Putri, Dinda Buana. “Kominfo Resmi Terbitkan Surat Edaran Menteri Tentang Etika Kecerdasan Buatan Atau Artificial Intelligent.” VOI, 2023. https://voi.id/teknologi/341605/kominfo-resmi-terbitkan-surat-edaran-menteri-tentang-etika-kecerdasan-buatan-atau-artificial-intelligent.

Putri, Diva Lufiana. “Isi SE Menkominfo soal Etika Penggunaan AI, Pelaku Tunduk UU ITE dan UU PDP.” kompas.com, 2023. https://amp.kompas.com/tren/read/2023/12/23/110000665/index.html?

Rabiah, Diva. “Polda Jatim Ungkap Penipuan Deepfake 3 Gubernur Jualan Motor.” Nasional. metro tv news, 30 April 2025. https://www.metrotvnews.com/play/kWDCnnVz-polda-jatim-ungkap-penipuan-deepfake-3-gubernur-jualan-motor.

Redaksi. “Analisis Maqashid Syari’ah Perspektif Imam Al-Ghazali dan Imam Al-Syatibi.” majelistabligh.id, 2024. https://majelistabligh.id/analisis-maqashid-syariah-perspektif-imam-al-ghazali-dan-imam-al-syatibi/3/.

Riyanto, Galuh Putri. “Kominfo Terbitkan SE yang Atur Etika Penggunaan AI.” kompas.com, 2023. https://tekno.kompas.com/read/2023/12/22/15520497/kominfo-terbitkan-se-yang-atur-etika-penggunaan-ai.

Rohman, Fathnur. “Keraton Kasepuhan menghadirkan Museum ‘Cave AI’ untuk wisata sejarah.” Antara News, 2024. https://www.antaranews.com/berita/4423793/keraton-kasepuhan-menghadirkan-museum-cave-ai-untuk-wisata-sejarah.

Safitri, Eva. “Diteken Jokowi, Revisi UU ITE Jilid II Resmi Berlaku.” detiknews.com, 2024. https://news.detik.com/berita/d-7123630/diteken-jokowi-revisi-uu-ite-jilid-ii-resmi-berlaku.

Sandon, Nicola, Valeria Specchio, dan Silvio Mario Cucciarrè. “Italy Leads the Way: The First National Law on Artificial Intelligence Is Approved.” RODL, 2025. https://www.roedl.it/en-gb/it/insights/pages/legal-newsletter/9-2025/italy-leads-way-first-national-law-artificial-intelligence-approved.aspx.

Sarzana. “New Cybercrimes.” Attorney At Law, 2025. https://www.lidis.it/en/i-nuovi-reati-informatici.

Septiyati Liman, Uyu. “VIDA catat penipuan ‘deepfake’ di Indonesia melonjak 1.550 persen.” ANTARA NEWS, 2024. https://www.antaranews.com/berita/4437365/vida-catat-penipuan-deepfake-di-indonesia-melonjak-1550-persen.

Setiawan, Felina Evangelica. “Surat Edaran Menkominfo Tentang Etika AI: Apa dan Mengapa?” Visiniaga, 2025. https://www.visiniaga.com/blog/our-blog-1/surat-edaran-menkominfo-tentang-etika-ai-apa-dan-mengapa-108?

Sibera, Mira. “Memahami UU PDP: Pelindungan Data Pribadi di Indonesia.” SiberMate, 2024. https://sibermate.com/hrmi/memahami-uu-pdp-pelindungan-data-pribadi-di-indonesia.

SIP Corp. “Deepfake Crimes in Indonesia: Legal Challenges and Criminal Liability in the AI Era.” SIP LAW FIRM, 2025. https://siplawfirm.id/deepfake-crimes-in-indonesia/.

Sitompul, Josua. “Wajah Baru UU ITE.” kompas.com, 2024. https://nasional.kompas.com/read/2024/01/05/06000061/wajah-baru-uu-ite?page=all.

Styanto, Mahfud Febry. “Potensi Positif Deepfake: Teknologi Sintesis Wajah untuk Edukasi, Perfilman, dan Pelestarian Budaya.” iBenews, 2025. https://www.ibenews.id/teknologi/2056033315/potensi-positif-deepfake-teknologi-sintesis-wajah-untuk-edukasi-perfilman-dan-pelestarian-budaya.

Tim Hukum Online. “Mengenal Tujuan dan Tingkatan 5 Maqashid Syariah.” Hukumonline.com, 2024. https://www.hukumonline.com/berita/a/maqashid-syariah-lt65c063a25e4c6/.

Wicaksana, Pradnya. “Pakar Hukum Siber UNAIR: Indonesia Harus Meratifikasi Budapest Convention.” unair.ac.id, 12 September 2022. https://unair.ac.id/pakar-hukum-siber-unair-indonesia-harus-meratifikasi-budapest-convention/.

Woll, Cornelia. “Regulation.” Dalam Britannica. 2025. https://www.britannica.com/topic/regulation.

Yoe, Bernard. “AI Deepfake : Manfaat atau Bahaya?” kumparan.com, 2024. https://kumparan.com/bernardyoe/ai-deepfake-manfaat-atau-bahaya-23jqGNHsLj9.

Zaenudin, Muhammad. “Mengenal Teknologi Deepfake, Berikut Manfaat dan Dampak Negatif yang Dapat Ditimbulkan.” kompas.com, 2024. https://www.kompas.com/tren/read/2024/09/13/084500565/mengenal-teknologi-deepfake-berikut-manfaat-dan-dampak-negatif-yang-dapat?page=all&_gl=11qdqlfu_gaMjE3NTQwMDg5LjE3NDQzNTk3NDA._ga_77DJNQ0227*MTc2Mzk3NDU1MS4xLjAuMTc2Mzk3NDczOC4wLjAuMA..#page2.

DAFTAR RIWAYAT HIDUP

Nama	:	Yasmine Nawal Choiry Zavier
Tempat Tanggal Lahir	:	Malang, 01 Maret 2003
Jenis Kelamin	:	Perempuan
Agama	:	Islam
Kewarganegaraan	:	Indonesia
Alamat	:	Jl. Ciliwung Airdas, No. 07, RT. 09, RW. 07, Kelurahan Purwantoro, Kecamatan Blimbing, Kota Malang
Email	:	yasminenawal01@gmail.com

Riwayat Pendidikan :

- TK Al-Wildaan : 2008 - 2010
- SDN Purwantoro 1 : 2010 - 2016
- SMP Putri Al-Irsyad Al-Islamiyyah : 2016 - 2019
- MA Putri Attaraqqie : 2019 – 2022
- UIN Maulana Malik Ibrahim Malang : 2022 - 2026