

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan ilmu pengetahuan dan teknologi telah memasuki segala bidang kehidupan manusia, seperti bidang pendidikan, kesehatan dan ekonomi. Pada khususnya di sektor perbankan. Dunia perbankan saat ini dan seterusnya akan terus berlanjut mendapatkan tantangan untuk bisa memberikan pelayanan yang baik dan bermanfaat bagi semua konsumen. Untuk menciptakan layanan dengan mudah, cepat, efisien dan sehingga dia bisa menjadi tolak ukur kemajuan atau tidak suatu negara dimana dia bisa diukur dengan tingkat pertumbuhan ekonomi, demikian pula layanan perbankan merupakan hal terpenting sebagai tolak ukur perkembangan dan kemajuan ekonomi suatu negara.¹

Kejahatan Siber atau juga dikenal sebagai *cyber crime*, merujuk pada serangkaian aktivitas kriminal yang dilakukan melalui penggunaan teknologi informasi dan jaringan komputer (*cyber space*). Kejahatan ini mencakup berbagai jenis tindakan yang memiliki tujuan merugikan atau menipu individu, organisasi, atau entitas lain, serta seringkali melibatkan penggunaan teknologi komputer, jaringan, dan internet. Secara sempit, kejahatan siber atau *cyber crime* di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

¹ Nur Kholis, *Perbankan Dalam Era Baru Digital*, Jurnal Economicus, Vol.12, No.1, 2018, h. 81.

Barda Nawawi Arief menggunakan istilah tindak pidana mayantara (*cybercrime*) untuk menunjuk jenis kejahatan ini yang terjadi dalam ruang siber (*cyberspace*).² Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik yang artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang itu dilakukan dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, ataupun pornografi dapat termasuk dalam kategori tindak pidana siber dalam arti luas.³

Kecerdasan buatan atau *Artificial Intelligence* (AI) berkembang dengan pesat dalam zaman sekarang, teknologi yang tumbuh dan berkembang sudah banyak yang menggunakan kecerdasan buatan, *artificial Intelligence* tidak hanya dalam wujud sebuah *robot humanoid*, banyak hal juga *artificial Intelligence* yang berwujud sistem komputer yang dikenal dengan *copilot* pada operasi sistem penggunaan *windows*, operasi sistem yang digunakan dalam sebuah *gadget* atau *smartphone* contoh *siri*, *google* dan *bixbie software* yang bisa diunggah, dan diprogramkan guna mengambil keputusan serta untuk berifikir dengan khalayak seorang manusia. *Artificial Intelligence* ini merupakan program yang diciptakan melalui sebuah bahasa *komputer* atau *Coding*.⁴

² Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2010, h. 253.

³ Vidya Prahassacitta, *Konsep Kejahatan Siber Dalam Sistem Hukum Indonesia*, 19 Juni 2019, Binus Universiti (*Online*), diakses <https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/>, diakses pada tanggal 2 Februari 2026.

⁴ Musfala Yudha, *Perlindungan Hukum Terhadap Data Pribadi Korban Pornografi Dengan Penggunaan Deepfake*, Skripsi, Institut Ilmu Sosial dan Bisnis Andi Sapada, Sulawesi Selatan, 2024, h. 1.

Teknologi kecerdasan buatan (*Artificial Intelligence*) telah berkembang dengan sangat pesat. Seperti berbagai inovasi lainnya, kecerdasan buatan membawa dampak positif maupun negatif. Salah satu dampak negatif yang muncul akibat kemajuan ini adalah kemudahan dalam memalsukan identitas melalui salah satu produk kecerdasan buatan, yaitu *deepfake*.⁵ *Deepfake* merupakan teknologi kecerdasan buatan yang digunakan untuk memanipulasi atau menipu suatu objek baik berupa suara, gambar, ataupun video.

Teknologi *deepfake* pertama kali mendapatkan perhatian dunia di tahun 2017 lalu,⁶ di mana saat itu Mantan Presiden Amerika Serikat yaitu Barrack Obama membuat pernyataan di internet yang ternyata tidak pernah ia lakukan. Hal serupa juga terjadi pada Presiden Joko Widodo mengenai video yang sangat viral di aplikasi TikTok, di mana saat itu Presiden Joko Widodo bernyanyi lagu Cupid dari *Girl Band* asal Korea, *Fifty-Fifty*, yang mana ini merupakan hasil dari teknologi kecerdasan buatan, yang menggantikan suara penyanyi asli dengan Presiden Joko Widodo, dan hasilnya adalah seperti Presiden Joko Widodo benar-benar menyanyikan lagu tersebut.

Istilah *deepfake* berasal dari gabungan kata *deep learning* dan *fake* (palsu).⁷ Istilah ini muncul di tahun 2017 ketika seorang pengguna Reddit bernama

⁵ Muhammad Hanan Nuhi, dkk, *Pembaharuan Hukum Penanganan Tindak Pidana Pemalsuan Identitas Akibat Penyalahgunaan Artificial Intelligence di Indonesia*, Jurnal BATAVIA, Vol.1, No.02, 2024, h. 80.

⁶ Jeremiah Maximillian Laza dan Rizky Karo Karo, *Perlindungan Hukum terhadap Artificial Intelligence dalam Aspek Penyalahgunaan Deepfake Technology pada Perspektif UU PDP dan GDPR (Legal Protection of Artificial Intelligence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR)*, Jurnal Lex Prospicit, Vol.1, No.2, 2023, h. 136.

⁷ F. Hardiman, *ISC Gelar Diskusi Potensi Ancaman Deepfake Image Jelang Pilpres 2024*, 1 Maret 2026, Indonesia Satu.com (Online), diakses melalui: <https://indonesiasatu.co/detail/isc-gelar-diskusi-potensi-ancaman-deepfake-image-jelang-pilpres-2024>, diakses pada tanggal 02 Februari 2026.

Deepfakes membagikan konten video dewasa di mana wajah pemeran aslinya telah diganti dengan wajah berbagai selebriti Hollywood.⁸ *Deepfake* digunakan untuk membuat konten manipulatif, biasanya berupa video atau audio, yang tampak atau terdengar seolah-olah berasal dari sumber asli, tetapi sebenarnya dibuat secara sintetis atau palsu. Jadi teknik *deepfake* ini memungkinkan seseorang untuk mengganti wajah aktor asli dalam video dengan wajah orang lain atau menciptakan situasi yang tidak pernah terjadi dalam realitas.

Ada dua metode untuk membuat *deepfake*, pertama yaitu menggunakan algoritma *Artificial Intelligence* bernama *encoder*. Pertama-tama, kita harus mengumpulkan ribuan foto dari dua orang yang berbeda. Lalu, *encoder* akan memprosesnya untuk menemukan kemiripan dan memancarkan wajah A ke wajah B di video lain. Selain *encoder*, *deepfake* juga bisa dibuat menggunakan *Generative Adversarial Network* atau GAN yang menggunakan komponen *generator* dan *discriminator* untuk menghasilkan data sintesis.⁹

Pada era digital sekarang, teknik *deepfake* atau menyunting wajah aktor atau pemeran dalam suatu video sudah sangat mudah dilakukan setiap orang tanpa perlu pembelajaran khusus. Sudah banyak aplikasi-aplikasi yang dapat melakukan teknik *deepfake* hanya dengan memasukan foto wajah yang diinginkan. Contoh aplikasi edit video yang sangat mudah diakses dan digunakan adalah aplikasi Capcut, dimana disediakan fitur *template* atau *templat* yang sudah terformat hanya

⁸ Anastasya Lavenia, *Deepfake Teknologi Pengganti Wajah Yang Menyimpan Bahaya*, CXO Media (Online), diakses melalui: <https://www.cxomedia.id/general-knowledge/20220616114747-55-175236/deepfake-teknologi-pengganti-wajah-yang-menyimpan-bahaya>, diakses pada tanggal 2 Februari 2026.

⁹ *Ibid.*

dengan memasukkan foto yang diinginkan makan fitur tersebut akan menyesuaikan dan melakukan teknik *deepfake* dengan sendirinya.

Ada juga teknologi kecerdasan buatan (*Artificial Intelligence*) yang ada pada aplikasi Telegram. Teknologi tersebut disediakan atau dibuat oleh seseorang yang memanfaatkan aplikasi komunikasi seperti Telegram dengan menggunakan *Bot Internet* atau program Internet yang di program untuk secara otomatis melakukan teknik *deepfake* terhadap gambar atau foto seseorang yang nantinya akan diedit sesuai keinginan atau kemampuan program tersebut. Sayangnya kebanyakan program tersebut dibuat untuk melakukan teknik *deepfake* yang berunsur pornografi.

Di Indonesia sendiri telah terjadi kasus penyalahgunaan teknologi *deepfake*, yang salah satunya yaitu terjadi pada tokoh publik sekaligus artis, Nagita Slavina. Di tahun 2022 lalu beredar sebuah video yang menampilkan seseorang diduga mirip tokoh publik sekaligus artis Nagita Slavina. Video yang berdurasi 61 (enam puluh satu) detik itu menampilkan adegan tidak senonoh di mana pelakunya memiliki wajah mirip tokoh publik sekaligus artis, Nagita Slavina.¹⁰

Hal tersebut merupakan *deepfake* pornografi hasil rekayasa menggunakan teknologi *deepfake*. Kemudian hal serupa dialami oleh belasan siswi alumni salah satu Sekolah Menengah Pertama (SMP) Negeri di Malang yang terjadi pada tahun 2021. Sebanyak 16 (enam belas) pelajar putri yang diduga berusia antara 14 (empat belas) hingga 18 (delapan belas) tahun datang ke Mapolresta Malang Kota

¹⁰ Zulfikar Hardiansyah, *Selebriti dan Tokoh Publik yang Jadi Korban Video Deepfake Selain Nagita Slavina*, Reska K. Nistanto, 19 Januari 2022, Kompas.com (Online), diakses melalui: <https://tekno.kompas.com/read/2022/01/19/13160047/selebriti-dan-tokoh-publik-yang-jadi-korban-video-deepfake-selain-nagita?page=all>, diakses pada tanggal 2 Februari 2026.

dan mengadu telah menjadi korban praktik *deepfake* konten video porno. Pelaku mengedit foto wajah para korban ke dalam video film dewasa sehingga seolah-olah mereka yang memerankan adegan syur tersebut.¹¹

Kasus-kasus penyalahgunaan teknologi ini sangat banyak terjadi dan kebanyakan korbannya bahkan tidak mengetahui bahwa dirinya adalah korban penyalahgunaan kecerdasan buatan untuk membuat konten pornografi. Tentunya sulit untuk mengetahui apabila masyarakat biasa yang menjadi korban dan bukan tokoh publik yang terkenal sehingga menimbulkan kehebohan apabila mereka menjadi korban dari penyalahgunaan teknologi *deepfake* untuk konten pornografi. Terlebih dalam kebebasan bersosial media dimana banyak media sosial yang bisa diakses tanpa perlu menyertakan identitas diri sehingga apabila seorang pengguna melakukan tindak kejahatan maka sangat sulit untuk melacak pelaku ataupun mendapatkan pembuktian karna adanya perlindungan privasi yang langsung disediakan oleh aplikasi tersebut.

Di Indonesia sendiri isu hukum normatif terkait *deepfake* berpusat pada kekosongan regulasi (*legal vacuum*) yang secara spesifik mendefinisikan dan mengatur manipulasi digital berbasis kecerdasan buatan dalam satu payung hukum yang komprehensif. Secara normatif, tantangan utama terletak pada ketidakpastian kualifikasi delik; apakah *deepfake* harus dipandang sebagai tindak pidana pemalsuan informasi secara murni (sebagaimana konstruksi Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik), ataukah sebagai bentuk

¹¹ Ahmad Yani, *Jadi Korban Deepfake Video Syur, Pelajar di Malang Lapor Polisi*, 10 Mei 2024, Radar Malang (Online), diakses melalui: <https://radarmalang.jawapos.com/kota-malang/811076448/jadi-korban-deepfake-video-syur-pelajar-di-malang-lapor-polisi>, diakses pada tanggal 2 Februari 2026.

baru pelanggaran hak atas integritas tubuh dan data biometrik yang bersifat personal.

Selain itu, problematika normatif muncul dalam aspek pertanggungjawaban pidana (*criminal liability*) yang masih terpaku pada subjek hukum manusia (*natuurlijke persoon*). Hukum positif saat ini kesulitan menjangkau area abu-abu mengenai tanggung jawab hukum pengembang perangkat lunak kecerdasan buatan, penyedia platform distribusi, hingga pengguna akhir dalam skenario di mana konten *deepfake* dihasilkan secara otomatis atau melalui *open-source*. Ketidaksinkronan antara Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, dan Undang-Undang Hak Cipta dalam mendefinisikan “orisinalitas” dan “kepemilikan identitas digital” menciptakan standar ganda dalam penegakan hukum, yang pada akhirnya menuntut adanya pembaruan hukum (naskah akademik baru) yang mampu mengakomodasi sifat anonimitas dan otomatisasi teknologi generatif ini.

Dari uraian latar belakang tersebut penulis tertarik untuk melakukan sebuah penelitian dalam bentuk skripsi dengan judul : Pertanggungjawaban Pidana Atas Rekayasa Konten Digital Berbasis Kecerdasan Buatan (*Deepfake*) Di Indonesia.

1.2. Rumusan Masalah

Dari rangkaian latar belakang masalah yang telah di uraikan di atas dapat di rumuskan masalah yang hendak dikaji adalah :

1. Bagaimanakah pengaturan hukum positif di Indonesia dalam mengatur rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) ?

2. Bagaimanakah bentuk pertanggungjawaban pidana yang tepat diterapkan terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia ?

1.3. Tujuan Penelitian

Adapun dalam penelitian ini merupakan sebuah kegiatan yang bertujuan sebagai berikut :

1. Untuk mengetahui dan memahami mengenai pengaturan hukum positif di Indonesia dalam mengatur rekayasa konten digital berbasis kecerdasan buatan (*deepfake*).
2. Untuk mengetahui dan memahami mengenai bentuk pertanggungjawaban pidana yang tepat diterapkan terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia.

1.4. Manfaat Penelitian

Melalui penelitian ini diharapkan dapat memberikan manfaat dalam ilmu pengetahuan hukum, baik secara teoritis maupun secara praktis, yaitu:

1. Secara teoritis penelitian ini dapat memberikan kontribusi pemikiran dalam rangka pengembangan khasanah ilmu pengetahuan khususnya dibidang hukum mengenai pertanggungjawaban pidana atas rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia.
2. Secara praktis penelitian ini dapat menjadi salah satu landasan hukum, rujukan dan/atau referensi sesuai ketentuan hukum mengenai pertanggungjawaban pidana atas rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia.

1.5. Tinjauan Pustaka

Dalam penelitian skripsi ini, peneliti menggali informasi dari pendapat para ahli hukum, teori-teori, asas-asas hukum dan beberapa peraturan yang menjadi konstruksi berfikir dalam menjawab pokok permasalahan.

1.5.1. Landasan Konseptual

Landasan konseptual merupakan suatu pengarah, atau pedoman yang lebih konkrit berisikan konsep-konsep umum atau tinjauan umum ketentuan dan pengertian serta hal hal yang berhubungan dengan pokok penelitian, adapun landasan konseptual dalam penelitian ini yaitu: a) Kejahatan Siber (*Cyber Crime*); b) Data Pribadi dan Privasi; c) Rekayasa Konten Digital Berbasis Kecerdasan Buatan (*Deepfake*).

1.5.1.1. Kejahatan Siber (*Cyber Crime*)

Membahas masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apabila jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi tersebut harus selalu dimutaakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya (*cyber crime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Untuk lebih mendalam ada beberapa pendapat tentang apa yang dimaksud dengan *cyber crime*.

Menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.¹²

Perkembangan teknologi informasi telah menggeser paradigma para ahli hukum dalam memberikan definisi dari kejahatan komputer, diawalnya para ahli hanya terfokus pada alat dan perangkat keras, yaitu komputer. Namun berkembangnya teknologi seperti internet, maka fokus dari definisi *cyber crime* adalah aktivitas yang dapat dilakukan di dunia siber melalui sistem informasi yang digunakan, sebagaimana yang diutarakan oleh Barda Nawawi Arief dengan kejahatan mayantara. Pada perkembangannya internet ternyata membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak terpikirkan akan terjadi. Sebuah teori menyatakan, *crime is product of society its self*, yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan.

Pada dasarnya *cyber crime* merupakan kegiatan yang memanfaatkan komputer sebagai sarana atau media yang didukung oleh sistem telekomunikasi, baik menggunakan telepon atau *wireles system* yang menggunakan antena khusus yang nirkabel. Hal inilah yang disebut “telematika” yaitu konvergensi antar teknologi telekomunikasi, media dan informatika yang semula masing-masing berkembang secara terpisah.

¹² Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT Refika Aditama, Jakarta, 2005, h. 40.

Widodo menjelaskan *cyber crime* dapat dibedakan menjadi 2 (dua) kategori, yaitu *cyber crime* dalam arti sempit dan *cyber crime* dalam arti luas. *Cyber crime* dalam arti sempit adalah kejahatan terhadap sistem komputer, sedangkan dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan komputer.¹³

Menurut Abdul Wahid dan M. Labib, *cyber crime* memiliki beberapa karakteristik, yaitu:¹⁴

1. Perbuatan yang dilakukan secara *illegal*, tanpa hak atau tindakan etis terjadi diruang/wilayah siber, sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya;
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet;
3. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
4. Pelakunya adalah orang yang menguasai penggunaan internet dan aplikasinya; dan
5. Perbuatan tersebut sering dilakukan secara transnasional.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokkan dalam bentuk, antara lain, yaitu:¹⁵

1. *Unauthorized Access to Computer System and Service*, yaitu kejahatan yang dilakukan dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet;

¹³ Widodo, *Sistem Pemidanaan Dalam Cyber Crime*, Laksbang Meditama, Yogyakarta, 2009, h. 24.

¹⁴ Abdul Wahid dan Mohammad Labib, *Op.Cit.*, h. 76.

¹⁵ Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Kharisma Putra Utama, Jakarta, 2013, h. 51.

2. *Illegal Contents*, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum;
3. *Data Forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku;
4. *Cyber Espionage*, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau data-data pentingnya tersimpan dalam suatu sistem komputerisasi;
5. *Cyber Sabotage and Extortion*, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan, atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet;
6. *Offence Against Intellectual Property*, yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Contohnya peniruan tampilan *web page* suatu situs milik orang lain secara ilegal; dan
7. *Infringements of Privacy*, yaitu kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.

Adapun jenis-jenis *Cyber Crime* berdasarkan motifnya, yaitu:¹⁶

- a. *Cyber Crime* sebagai tindak kejahatan murni;
Dimana orang yang melakukan kejahatan yang dilakukan secara di sengaja. Contohnya pencurian, tindakan anarkis terhadap suatu sistem informasi atau sistem komputer.
- b. *Cyber Crime* sebagai tindakan kejahatan abu-abu;
Dimana kejadian ini tidak jelas antara kejahatan kriminal atau bukan, karena pelaku melakukan pembobolan tetapi tidak merusak, mencuri, atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer.
- c. *Cyber Crime* yang menyerang individu;
Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, contohnya pornografi, *cyber stalking*, dan lain-lain.
- d. *Cyber Crime* yang hak cipta (hak milik); dan

¹⁶ *Ibid*, h. 54.

Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/non-materi.

e. *Cyber Crime* yang menyerang pemerintah.

Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan.

1.5.1.2. Data Pribadi dan Privasi

Setiap informasi privat adalah data pribadi, namun tidak semua informasi pribadi merupakan bagian dari privasi individu. Data berasal dari bahasa Latin jamak yang berarti “apa yang diberikan”.¹⁷

Beberapa ahli juga telah mendefinisikan definisi data, Menurut Nuzulla Agustina, data merupakan serangkaian angka, fakta, gambar, diagram, kata, simbol, karakter, dan sebagainya mengenai suatu hal yang sering terjadi yang menyampaikan sebuah pemikiran, kondisi, objek, atau situasi. Selain Nuzra, menurut Arikunto Suharsimi, data merupakan sekumpulan informasi dan angka yang dapat digunakan sebagai dasar untuk menyusun informasi.¹⁸

Menurut pakar E. Mutiara dan Kuswwadi, data adalah sekumpulan informasi yang didapat dari suatu pengamatan dan dapat berupa simbol, angka atau karakteristik.¹⁹ Selain itu, pada tahun 2008, negara-negara anggota Uni Eropa menetapkan *General Data Protection Rule* yang mendefinisikan data pribadi sebagai informasi yang dapat mengidentifikasi

¹⁷ Anggen Suari, K. R., & Sarjana, I. M., *Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia*, Jurnal Analisis Hukum, Vol.6, No.1, 2023, h. 132.

¹⁸ Rifqi Mulyawan, *Ini Dia Sebenarnya Pengertian Data: Menurut Ahli, Sejarah, Fungsi, Jenis, dan Contohnya*, 26 Oktober 2024, Rifqi Mulyawan.Com (Online), diakses melalui: <https://rifqimulyawan.com/blog/pengertian-data/>, diakses pada tanggal 2 Februari 2026.

¹⁹ *Ibid.*

seseorang yang berkaitan dengan tanda pengenal seperti nama, nomor identifikasi, lokasi individu, data fisik, data fisiologis, identitas, dan lainnya.

Data pribadi merupakan informasi mengenai individu yang mencakup fakta-fakta, komunikasi, serta pendapat yang memiliki keterkaitan dengan orang tersebut dan dirasakan sebagai informasi sensitif, sehingga pengumpulan, penggunaan, atau distribusinya dianggap terbatas atau dilarang.²⁰ Sebenarnya, data pribadi dan privasi adalah dua hal yang saling terkait dan tidak dapat dipisahkan. Meskipun mereka memiliki variasi dalam lingkup serta ketentuan substansinya.

Maka dapat disimpulkan bahwa data pribadi adalah informasi yang berkaitan dengan individu yang mencakup fakta, komunikasi, dan opini yang memiliki keterkaitan antar orang, di mana bersifat sensitif serta dibatasi dalam pengumpulan, penggunaan, dan distribusinya. Pada dasarnya, data pribadi seringkali berupa informasi tentang seseorang seperti jenis kelamin, alamat tempat tinggal, pendidikan, dan rincian pribadi, yang ketika dikumpulkan dapat membentuk profil individu untuk menghasilkan informasi tertentu.

1.5.1.3. Rekayasa Konten Digital Berbasis Kecerdasan Buatan (*Deepfake*)

Deepfake bukan sekedar teknologi melainkan dapat menimbulkan potensi ancaman. Era digital yang canggih telah membawa perubahan dalam berkomunikasi, berinteraksi dan memahami realitas, namun teknologi juga dapat menimbulkan ancaman yang serius, terutama penggunaan untuk

²⁰ Shofiyah, E. N., & Indri Fogar, S., *Penyalahgunaan Data Pribadi Penerima Pinjaman Dalam Peer To Peer Lending*, Novum: Jurnal Hukum, Vol.6, No.2, 2019, h. 2.

menyebarkan informasi palsu, melakukan penipuan maupun merusak reputasi seseorang. Salah satu kemajuan teknologi yang mencolok adalah kemampuan untuk menciptakan konten yang sangat realistis yaitu teknologi *deepfake*.

Deepfake berasal dari Bahasa Inggris yaitu “*deep learning*” (pembelajaran secara mendalam) dan kata *fake* (palsu). *Deepfake* dapat memanipulasi fitur wajah dan audio seseorang melalui *artificial intelligence*. Perkembangan teknologi *deepfake* membawa ancaman serius yang signifikan dikarenakan dapat digunakan untuk menyebarluaskan informasi palsu secara serta berpotensi besar untuk mempengaruhi opini publik.²¹

Penyalahgunaan aplikasi *deepfake* dapat dikriminalisasi apabila terjadi penyalahgunaan untuk melindungi hak-hak individu dan mencegah dampak negatif yang lebih luas akibat penyalahgunaan teknologi tersebut hal ini dapat memicu kerugian nyata pada individu atau kelompok sehingga menimbulkan potensi adanya korban.

Marissa Koopman, Andrea Macarulla Rodriguez, dan Zeno Geradts pada jurnalnya memberikan penerangan pada *Deepfake Technology* sebagai algoritma, berupa: “*The deepfake algorithm allows a user to switch the face of one actor in a video with the face of a different actor in a photorealistic manner*”.²² Hal ini menjelaskan bahwa mengenai “*Algoritma Deepfake*

²¹ Juefei-Xu, et.al., *Countering Malicious Deepfakes: Survey, Battleground, and Horizon*, 2015, h. 65.

²² Andrea Macarulla Rodriguez Marissa Koopman, *Detection of Deepfake Video Manipulation*, Zeno Geradts University of Amsterdam & Netherlands Forensic Institute, 2018, h. 64.

memungkinkan pengguna untuk mengganti wajah satu aktor dalam video dengan wajah aktor berbeda secara fotorealistik”. Teknologi *deepfake* menggunakan algoritma *machine learning* dan jaringan saraf tiruan yang digunakan untuk memanipulasi atau menggantikan wajah seseorang dalam video atau gambar dengan tingkat akurasi dan kemiripan yang hampir sempurna.

1.5.2. Landasan Yuridis

Landasan yuridis merupakan dasar hukum yang mengatur dan berhubungan dengan objek penelitian. Landasan yuridis yang dapat digunakan untuk menjelaskan isu yang akan dibahas. Adapun landasan yuridis dalam penelitian ini yakni:

1. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dalam Pasal 28G ayat (1) mengenai hak atas perlindungan diri pribadi, kehormatan, dan martabat. Pasal 28F mengenai hak memperoleh dan menyampaikan informasi. *Deepfake* berpotensi melanggar hak atas kehormatan dan privasi seseorang, sehingga memiliki dimensi konstitusional.
2. Kitab Undang-Undang Hukum Pidana dalam Pasal 310 sampai dengan Pasal 311 mengenai Pencemaran nama baik. Pasal 378 mengenai Penipuan. Pasal 263 mengenai Pemalsuan. *Deepfake* dapat dikualifikasikan sebagai bentuk pemalsuan atau penipuan apabila memenuhi unsur delik.

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 sebagaimana Pasal yang relevan diantaranya Pasal 27 ayat (1) mengenai konten asusila. Pasal 27 ayat (3) mengenai pencemaran nama baik. Pasal 28 ayat (1) mengenai berita bohong. Pasal 35 mengenai manipulasi informasi elektronik. *Deepfake* sangat relevan dikaitkan dengan Pasal 35 tentang manipulasi informasi elektronik. Dan mengenai Undang-Undang ini terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
4. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi. *Deepfake* pornografi dapat dijerat dengan ketentuan produksi dan distribusi konten pornografi.
5. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Wajah dan suara termasuk data biometrik yang dilindungi. Penggunaan tanpa persetujuan dapat dikenakan sanksi administratif maupun pidana.

Berdasarkan landasan yuridis yang berlaku di Indonesia, pertanggungjawaban pidana atas rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) pada dasarnya dapat dikonstruksikan melalui ketentuan peraturan perundang-undangan. Landasan yuridis yang ada menunjukkan bahwa hukum pidana Indonesia telah menyediakan instrumen

untuk menjerat pelaku penyalahgunaan *deepfake*, namun perkembangan teknologi yang semakin pesat menuntut adanya regulasi yang lebih spesifik guna menjamin kepastian hukum.

1.5.3. Landasan Teori

Landasan teori merupakan teori-teori yang digunakan oleh penulis sebagai dasar atau pedoman berpikir dalam penelitian. Adapun landasan teori dalam penelitian ini yakni: a) Teori Kesalahan (*Schuld*); b) Teori Penanggulangan Kejahatan; dan c) Teori Pertanggungjawaban Pidana.

1.5.3.1. Teori Kesalahan (*Schuld*)

Dalam kamus Bahasa Indonesia kesalahan diartikan sebagai : “Perihal salah, kekeliruan, dan kealpaan”.²³ Definisi-definisi tentang pengertian Kesalahan menurut para Ahli antara lain, yaitu:

1. Menurut Sukirman kesalahan adalah penyimpangan terhadap hal-hal yang benar yang sifatnya sistematis, konsisten maupun insidental pada daerah tertentu.²⁴
2. Menurut Soetrisno, kesalahan adalah suatu kejadian atau tingkah laku yang signifikan dapat diamati berbeda dari kejadian atau tingkah laku yang diharapkan.²⁵

²³ Departemen Pendidikan dan Kebudayaan, *Kamus Besar Bahasa Indonesia*, Balai Pustaka, Jakarta, 2011, h. 17.

²⁴ Wakhidatunisyak, *Analisis Kesalahan Menyelesaikan Soal Matematika Materi Himpunan Kelas VII D MTs Assyafi'fah Gondang Semester Genap Tahun Pelajaran 2011/2012*, Tulungagung, 2011, h. 16.

²⁵ Juliana Molle, *Analisis Kesalahan Jawaban Siswa Kelas V SDN Latihan SPG Ambon dalam Menyelesaikan Topik Geometri*, Ambon, 2000, h. 5.

3. Rosyidi mendefinisikan kesalahan adalah suatu bentuk penyimpangan terhadap hal yang dianggap benar atau prosedur yang ditetapkan sebelumnya.²⁶

Dari uraian diatas dapat disimpulkan bahwa kesalahan adalah ketidaksesuaian atau penyimpangan terhadap aturan atau prosedur yang sudah ditetapkan sebelumnya bersifat sistematis, konsisten dan insidental. Ada bermacam-macam bentuk kesalahan, dalam ilmu hukum mengenal dua bentuk kesalahan yaitu kesengajaan (*dolus*) dan kealpaan (*culpa*).²⁷ Kedua bentuk kesalahan tersebut juga sering kita temui pada lingkungan pendidikan dalam hal ini proses pembelajaran siswa. Berikut merupakan penjelasan dari bentuk-bentuk kesalahan yaitu kesengajaan dan kealpaan.

Dalam *Memori van Toeliching* dijelaskan maksud dari kesengajaan adalah *willens en watens* yang artinya menghendaki dan menginsyafi atau mengetahui.²⁸ Seseorang yang melakukan suatu perbuatan dengan sengaja harus menghendaki perbuatannya dan harus menginsyafi atau mengetahui akibat yang mungkin akan terjadi karena perbuatannya. Menurut Moeljatno kesengajaan adalah suatu pengetahuan, yang mana adanya suatu hubungan batin atau pikiran dengan perbuatan yang dilakukan oleh seseorang.²⁹

²⁶ Endah Dwi Utari, *Analisis Kesalahan Siswa Berdasarkan Watson's Error Category Dalam Menyelesaikan Soal Model PISA Ditinjau Dari Gaya Kognitif Field Dependent-Field Independent*, Surabaya, 2019, h. 9.

²⁷ Triyadi Gembel, *Pengertian Kesalahan Dalam Hukum Pidana*, 11 Juli 2013, Arsip Blog (Online), melalui: <http://triyadipkn.blogspot.com/2013/07/1pengertian-kesalahan-dalam-hukum-pidana.html>, diakses pada 2 Februari 2026.

²⁸ Gede Agastia Erlandia, *Penyelesaian Perkara Tindak Pidana Terkait Penghinaan Agama*, Jurnal Hukum, Vol.1, No.2, 2018, h. 543.

²⁹ *Ibid.*

Dalam kata lain kesengajaan berarti kehendak atau keinginan yang dilakukan dengan sengaja yang ditunjukan terhadap suatu tindakan.

Sedangkan kealpaan atau kelalaian yaitu suatu kesalahan sebagai akibat kurang berhati hati sehingga secara tidak sengaja sesuatu terjadi. Menurut Simons kealpaan terjadi karena tidak adanya kehati-hatian dan kurangnya perhatian terhadap akibat yang mungkin terjadi.³⁰ Dalam berbagai hal kealpaan atau kelalaian ini memiliki dampak atau akibat yang terjadi contohnya mengalami kecelakaan akibat tergesa-gesa dalam berkendara sepeda motor karena kurang kehati-hatian dalam berkendara tanpa berpikir panjang akibat yang akan terjadi.

Dari kedua bentuk kesalahan tersebut juga sering ditemukan dalam dunia pendidikan salah satunya siswa mengalami kesalahan dalam melakukan sesuatu baik secara sengaja atau tidak sengaja (kealpaan). Seperti halnya secara sengaja tidak mengerjakan soal yang diberikan karena merasa tidak bisa mengerjakan soal tersebut, dan tidak teliti dalam mengerjakan seperti menghitung karena kurangnya kehati-hatian dalam mengerjakan soal. Hal tersebut memberikan dampak negatif pada hasil belajar siswa karena kesalahan yang diperbuat.

1.5.3.2. Teori Penanggulangan Kejahatan

Kejahatan merupakan suatu tindakan yang bertentangan (*delviant behavior*) dengan nilai dan norma serta melekat (*inherent*) dalam setiap bentuk masyarakat yang telah disahkan oleh hukum tertulis. Upaya

³⁰ Triyadi, *Loc.Cit.*

Penanggulangan merupakan segala bentuk daya dan usaha yang dilakukan oleh setiap orang maupun Lembaga pemerintahan ataupun swasta yang bertujuan mengusahakan pengamanan, pengendalian dan kesejahteraan hidup sesuai dengan hak asasi manusia yang berlaku.

Menurut Barda Nawawi upaya atau kebijakan untuk pencegahan dan penanggulangan kejahatan termasuk bagian bidang kebijakan kriminal. Kebijakan penanggulangan kejahatan dilakukan dengan menggunakan sarana “penal” (hukum pidana) yang berfokus pada Langkah “*repressive*”, yaitu penindasan, pemberantasan, penumpasan sesudah kejahatan terjadi, oleh karena itu kebijakan hukum pidana khususnya pada tahap kebijakan yudikatif harus mempertimbangkan dan mengarah pada tercapainya tujuan dari kebijakan sosial berupa *social welfare* (kesejahteraan sosial) dan *social defence* (pertahanan sosial).³¹

Kebijakan penanggulangan kejahatan atau disebut dengan istilah “politik kriminal” meliputi ruang lingkup yang cukup luas, G. Peter Hoefnagels menggambarkan ruang lingkup “*criminal policy*” sebagai berikut, yaitu:³²

- a. Penerapan hukum pidana (*criminal law application*);
- b. Pencegahan tanpa pidana (*prevention without punishment*); dan
- c. Mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat media massa (*influencing views of society on crime and punishment/mass media*).

Upaya penganggulangan kejahatan dapat dibagi menjadi 2 (dua) yaitu, jalur “penal” (hukum pidana) dan “non penal” (diluar hukum pidana). Upaya *preventif* merupakan langkah langka yang dilakukan untuk mencegah terjadi atau timbulnya kejahatan yang pertama kali dilakukan, hal ini dikarenakan mencegah lebih baik daripada mendidik penjahat menjadi lebih

³¹ Hermansyah A, *Penanggulangan Kejahatan Dengan Pidana Badan di Indonesia*, Kanun Jurnal Ilmu Hukum, Vol.15, No.2, 2013, h. 192.

³² G. Peter Hoefnagels, *The Other Side of Criminology*, Dordrecht, Springer Netherlands, 1973, h. 34.

baik, seperti halnya sesuai dengan semboyan dalam kriminologi yang menyatakan bahwa usaha-usaha memperbaiki penjahat perlu diperhatikan dan harus diarahkan agar tidak terjadi lagi kejahatan yang sama. Upaya preventif diutamakan karena dapat dilakukan oleh siapa saja tanpa suatu keahlian khusus dan kemampuan finansial.³³

Barnest dan Teeters mengemukakan beberapa cara menanggulangi kejahatan yaitu:³⁴

- 1) Menyadari bahwa akan adanya kebutuhan untuk mengembangkan dorongan atau tekanan sosial dan tekanan ekonomi yang dapat mempengaruhi tingkah laku seseorang untuk melakukan perbuatan jahat; dan
- 2) Memusatkan perhatian kepada individu yang menunjukkan potensi kriminal atau sosial, meskipun potensi tersebut disebabkan oleh gangguan biologis dan psikologis atau kurang mendapat kesempatan sosial ekonomis yang baik.

Sedangkan upaya *represif* merupakan bentuk upaya penanggulangan kejahatan yang secara konsep digunakan setelah terjadi kejahatan. Tujuan upaya *represif* dimaksudkan untuk menindak lanjut para pelaku sesuai dengan kejahatan dan memperbaikinya agar pelaku sadar bahwa perbuatan yang dilakukannya merupakan perbuatan yang melanggar hukum dan merugikan masyarakat. Sehingga pelaku diharapkan untuk tidak mengulangi dan menghindari kejahatan yang sama maupun yang akan dilakukan mengingat sanksi yang akan ditanggung sangat berat.

Sistem represif tidak terlepas dari sistem peradilan pidana di Indonesia. Terdapat 5 (lima) sub-sistem yaitu: kehakiman, kejaksaan,

³³ Situmeang S.M.T., *Kebijakan Kriminal Dalam Penegakan Hukum Untuk Mewujudkan Keadilan Dalam Perspektif Hak Asasi Manusia*, Res Nullius Law Journal, Vol.1, No.1, 2019, h. 15.

³⁴ *Ibid.*

kepolisian, Lembaga permasyarakatan, dan kepengacaraan (advokat) yang merupakan serangkaian hubungan secara fungsional. Upaya represif dalam pelaksanaannya dilakukan dengan metode perlakuan (*treatment*) dan penghukuman (*punishment*).

1.5.3.3. Teori Pertanggungjawaban Pidana

Dalam hukum pidana dikenal istilah pertanggungjawaban, bahasa Belanda menyebutkan *toerekenbaarheid*, dalam bahasa Inggris *criminal responsibility* atau istilah lainnya *criminalliability*. Pertanggungjawaban “pertanggungjawaban pidana”, pidana, sedangkan Roeslan Saleh Moeljatno menyebut mengatakan “pertanggungjawaban dalam hukum pidana”, ahli hukum lainnya lebih banyak menyebutkan sebagai “pertanggungjawaban pidana”.³⁵

Pertanggungjawaban atau yang dikenal dengan konsep *liability* dalam segi falsafah hukum, Roscoe Pound menyatakan bahwa: *I..use simple word “liability” for the situation whereby one may exact legally and other is legally subjeced to the excaxtion*” pertanggungjawaban pidana diartikan Pound adalah sebagai suatu kewajiban untuk membayar pembalasan yang akan diterima pelaku dari seseorang yang telah dirugikan.³⁶ menurutnya juga bahwa pertanggungjawaban yang dilakukan tersebut tidak hanya menyangkut masalah hukum semata akan tetapi menyangkut pula masalah nilai-nilai moral ataupun kesusilaan yang ada dalam suatu masyarakat.

³⁵ Sampur Dongan Simamora & Mega Fitri Hertini, *Hukum Pidana Dalam Bagan*, FH Untan Press, Pontianak, 2015, h. 166.

³⁶ Romli Atmasasmita, *Perbandingan Hukum Pidana*, Mandar Maju, Bandung, 2000, h. 65.

Selain Roscoe Pound, Ada beberapa para ahli memberikan pengertian pertanggungjawaban pidana diantaranya, yaitu:

1. Simons mengatakan kemampuan bertanggungjawab dapat diartikan suatu keadaan psikis sedemikian rupa, sehingga penerapan suatu upaya pemidanaan, baik ditinjau secara umum maupun dari sudut orangnya dapat dibenarkan. Selanjutnya dikatakannya, seorang pelaku tindak pidana mampu bertanggungjawab apabila: Pertama, mampu mengetahui atau menyadari bahwa perbuatannya bertentangan dengan hukum. Kedua, mampu menentukan kehendaknya sesuai dengan kesadaran tadi.³⁷
2. Berbeda dengan Simons, Van Hamel memberikan pengertian pertanggungjawaban pidana adalah suatu keadaan normal psikis dan kemahiran yang membawa tiga macam kemampuan, yaitu pertama, mampu untuk dapat mengerti makna serta akibat sungguh-sungguh dari perbuatan perbuatan sendiri. Kedua, mampu untuk menginsyafi bahwa perbuatan perbuatan itu bertentangan dengan ketertiban masyarakat. Ketiga, mampu untuk menentukan kehendak berbuat.³⁸
3. Pompe memberikan pertanggungjawaban pidana dalam batasan unsur-unsur yaitu kemampuan berpikir pada pelaku yang memungkinkan menguasai pikirannya dan menentukan kehendaknya, pelaku dapat mengerti makna dan akibat dari tingkah lakunya serta pelaku dapat menentukan kehendaknya sesuai dengan pendapatnya (tentang makna dan akibat tingkah lakunya).³⁹

Apabila dilihat dari pendapat-pendapat para ahli tersebut diatas, pertanggungjawaban pidana berbeda dengan perbuatan pidana. Perbuatan pidana hanya menunjuk kepada dilarang dan diancamnya perbuatan dengan suatu pidana. Apakah orang yang melakukan perbuatan kemudian dijatuhi pidana, tergantung dari pada perbuatan tersebut mengandung kesalahan. Sebab asas dalam pertanggungjawaban hukum pidana adalah “tidak dipidana jika tidak ada kesalahan (*Geen straf zonder schuld; Actus non facit reum nisi mens sis rea*) yang artinya penilaian pertanggungjawaban pidana

³⁷ Teguh Prasetyo, *Hukum Pidana*, Raja Grafindo Persada, Depok, 2010, h. 85.

³⁸ Eddy O.S. Hiarij, *Prinsip-Prinsip Hukum Pidana*, Cahaya Atma Pustaka, Yogyakarta, 2014, h. 121.

³⁹ Teguh Prasetyo, *Op.Cit.*, h. 86.

itu ditujukan kepada sikap batin pelakunya, bukan penilaian terhadap perbuatannya. Pengecualian prinsip *actus reus* dan *mens rea* adalah hanya pada delik-delik yang bersifat *strict liability* (pertanggungjawaban mutlak), dimana pada tindak pidana yang demikian itu adanya unsur kesalahan atau *mens rea* tidak perlu dibuktikan.⁴⁰

Kesalahan dalam arti seluas-luasnya, dapat disamakan dengan pengertian pertanggungjawaban dalam hukum pidana. Didalamnya terkandung makna dapat dicelanya sipembuat atau perbuatannya. Jadi, apabila dikatakan bahwa orang itu bersalah melakukan sesuatu tindak pidana, maka itu berarti bahwa ia dapat dicela atas perbuatannya.

Berbicara masalah pertanggungjawaban pidana seperti hal nya diatas, berarti berbicara mengenai orang yang melakukan perbuatan pidana.⁴¹ ada dua pandangan mengenai pertanggungjawaban pidana, yaitu pandangan yang Monistis oleh Simon dan pandangan yang Dualistis oleh Herman Kotorowicz.

Menurut pandangan Monistis, unsur-unsur *strafbaar feit* itu meliputi baik unsur perbuatan yang lazim disebut unsur objektif, maupun unsur pembuat, yang lazim disebut unsur subjektif. Oleh karena dicampurnya unsur perbuatan dan unsur pembuatnya, maka dapatlah disimpulkan bahwa *strafbaar feit* adalah sama dengan syarat penjatuhan pidana, sehingga seolah-olah dianggap bahwa kalau terjadi *strafbaar feit*, maka pasti pelakunya dapat dipidana.⁴²

Maka dari itu para penganut pandangan monistis tentang *strafbaar feit* atau *criminal act* berpendapat, bahwa unsur-unsur pertanggungjawaban

⁴⁰ Hasbullah F. Sjawie, *Pertanggungjawaban Pidana Korporasi Pada Tindak Pidana Korupsi*, Prenada Media Group, Jakarta, 2015, h. 11.

⁴¹ Eddy O.S. Hiariej, *Op.Cit.*, h. 119.

⁴² Muladi & Dwidja Priyatno, *Pertanggungjawaban Pidana Korporasi*, Kencana Prenadamedia Group, Jakarta, 2010, h. 63

pidana yang menyangkut pembuat delik yang meliputi:⁴³ Pertama, Kemampuan bertanggungjawab, yaitu mampu memahami secara sungguh-sungguh akibat yang bertentangan dengan ketertiban masyarakat, Kedua, mampu untuk menginsyafi bahwa perbuatan itu bertentangan dengan ketertiban masyarakat dan mampu untuk menentukan kehendak berbuat. Ketiga kemampuan tersebut bersifat kumulatif. Artinya salah satu saja kemampuan bertanggungjawab tidak terpenuhi, maka seseorang dianggap tidak dapat dipertanggungjawabkan.⁴⁴

1.6. Penelitian Terdahulu

Dalam Penelitian ini terdapat beberapa penelitian terdahulu yang memiliki tema yang sama, namun memiliki fokus pembahasan yang berbeda, dan tentu saja penelitian yang sedang ditulis saat ini memiliki fokus pembahasan yang berbeda dari penelitian-penelitian terdahulu dan belum pernah ditulis sebelumnya. Sehingga, terlihat jelas bahwa penelitian yang dilakukan saat ini bukan pengulangan atau duplikasi dari kajian atau penelitian yang telah ada. Hal tersebut dapat ditelaah dari judul maupun isu pembahasan dari penelitian sebelumnya yang disajikan dalam bentuk tabel, sehingga agar lebih memudahkan untuk mengetahui perbedaannya, serta dapat memperlihatkan keaslian dari penelitian saat ini dengan penelitian sebelumnya, yaitu:

No	Keterangan	Uraian
1	Nama / Jenis Penelitian	Puteri Nurul Izzah / Skripsi, Universitas Islam Negeri Sunan Ampel Fakultas Syariah Dan Hukum Jurusan Hukum Publik Islam Program Studi Hukum Surabaya

⁴³ *Ibid*, h. 65.

⁴⁴ Eddy O.S. Hiarij, *Op.Cit.*, h. 128.

		2024.
	Judul	Analisis Yuridis Manipulasi Gambar <i>Deepfake</i> Pornografi
	Perbedaan	Hasil dari penelitian ini disimpulkan bahwasannya tindakan manipulasi gambar <i>deepfake</i> pornografi dapat dikategorikan sebagai tindak pidana pemalsuan. Tindakan pemalsuan gambar <i>deepfake</i> pornografi memuat unsur pidana pemalsuan, pornografi, dan kekerasan berbasis gender <i>online</i> .
2	Nama / Jenis Penelitian	Nabila Syahrani Lestari / Skripsi, Fakultas Hukum Universitas Sriwijaya 2024
	Judul	Kebijakan Formulasi Hukum Pidana Atas Praktik <i>Deepfake</i> Dilihat Dari Perspektif Kejahatan Siber Dan Pornografi
	Perbedaan	Hasil dari penelitian ini bahwa Indonesia tidak memiliki aturan khusus yang mengatur mengenai <i>deepfake</i> pornografi. Dimana Indonesia mengklasifikasikan <i>deepfake</i> atau kecerdasan buatan lainnya sebagai informasi elektronik sehingga Undang-Undang yang dikaitkan ialah Undang-Undang ITE. Namun untuk tindak pidana <i>deepfake pornografi</i> , selain Undang-Undang ITE dapat juga dikaitkan dengan Undang-Undang lain seperti KUHP, Undang-Undang Pornografi, Undang-Undang TPKS dan Undang-Undang PDP.
3	Nama / Jenis Penelitian	Moechamad Rizal Akbar / Skripsi, Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember Fakultas Syariah Jurusan Hukum Islam Program Studi Hukum Tata Negara Maret 2025.
	Judul	Perlindungan Hukum Tentang Hak Privasi Tubuh Manusia Terhadap <i>Deepfake</i> Oleh Kecerdasan Buatan (AI) Dalam Perspektif Hak Asasi Manusia.
	Perbedaan	Hasil penelitian ini adalah Perlindungan hukum hak privasi terhadap korban kejahatan <i>deepfake</i> visual oleh kecerdasan buatan dalam beberapa peraturan perundang-undangan seperti Undang-Undang PDP, Undang-Undang ITE, KUHP, dan Undang-Undang

		Pornografi, belum memberikan penjelasan secara definisi mengenai kejahatan <i>deepfake</i> sehingga dalam hal ini menjadi suatu kelemahan bagi penegak hukum di Indonesia.
4	Nama / Jenis Penelitian	Titin Patikasari / Skripsi, Program Studi Ilmu Hukum Fakultas Syariah Dan Hukum UIN Syarif Hidayatullah Jakarta 1446 H/2024 M.
	Judul	Pelindungan Hukum Bagi Korban <i>Deepfake</i> Pornografi (Studi Perbandingan Indonesia dan Korea Selatan)
	Perbedaan	Hasil penelitian menunjukkan bahwa Indonesia dan Korea Selatan belum memiliki peraturan komprehensif yang mengatur teknologi <i>deepfake</i> . Di Indonesia, pengaturan terkait <i>deepfake</i> pornografi diatur dalam Undang-Undang ITE, Undang-Undang Pornografi, Undang-Undang PDP, dan Undang-Undang TPKS. Sedangkan <i>deepfake</i> pornografi di Korea Selatan telah diatur dalam Undang-Undang Hukuman Kejahatan Kekerasan Seksual.

Penelitian ini memiliki persamaan dengan penelitian-penelitian sebelumnya yang sama-sama membahas tindak pidana siber dan pertanggungjawaban hukum atas penyalahgunaan teknologi digital dalam perspektif hukum positif Indonesia, khususnya yang dikaitkan dengan Undang-Undang Informasi dan Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana. Kesamaan tersebut terletak pada fokus kajian mengenai konstruksi pertanggungjawaban hukum terhadap pelaku, perlindungan hukum bagi korban, serta analisis norma hukum yang digunakan untuk menjerat perbuatan berbasis teknologi informasi. Selain itu, penelitian ini juga menggunakan pendekatan hukum normatif dengan menelaah peraturan perundang-undangan sebagai sumber hukum utama.

Penelitian ini memiliki perbedaan dengan penelitian sebelumnya karena secara khusus menitikberatkan pada rekayasa konten digital berbasis kecerdasan

buatan (*deepfake*) sebagai bentuk perkembangan terbaru dalam kejahatan siber, yang belum diatur secara eksplisit dalam peraturan perundang-undangan Indonesia. Jika penelitian terdahulu umumnya membahas tindak pidana siber seperti pencemaran nama baik, penipuan daring, atau penyebaran konten asusila berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, penelitian ini lebih fokus pada konstruksi pertanggungjawaban pidana terhadap manipulasi identitas digital berbasis teknologi kecerdasan buatan serta analisis kekosongan dan kekaburan norma dalam sistem hukum nasional. Dengan demikian, penelitian ini terdapat kebaruan dalam aspek objek kajian maupun pendekatan analisis normatifnya.

1.7. Metode Penelitian

Metode penelitian ini merupakan cara yang digunakan untuk mendapatkan data serta memperoleh jawaban yang akurat atas rumusan masalah diatas dengan mencari dan mengelola data dalam suatu penelitian.

1.7.1. Jenis Penelitian

Jenis penelitian ini adalah penelitian hukum normatif, penelitian hukum untuk menemukan aturan hukum, prinsip-prinsip hukum maupun doktrin-doktrin hukum. “Penelitian hukum normatif adalah proses penelitian untuk meneliti dan mengkaji tentang hukum sebagai norma, aturan, asas hukum, prinsip hukum, doktrin hukum, teori hukum dan kepustakaan lainnya untuk menjawab permasalahan hukum yang diteliti”.⁴⁵

⁴⁵ Suyanto, *Metode Penelitian Hukum Pengantar Penelitian Normatif Empiris dan Gabungan*, Cetakan Pertama, Unigres Press, Gresik, 2022, h. 88.

Hasil dari penelitian ini memberikan diskripsi mengenai rumusan masalah yang diajukan, penelitian normatif hanya meneliti norma hukum, tanpa melihat praktek hukum di lapangan (*law in action*) mengenai penelitian terkait pertanggungjawaban pidana atas rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia

1.7.2. Metode Pendekatan

Metode pendekatan merupakan salah satu tahapan penelitian yang dimaksudkan untuk mengumpulkan bahan-bahan hukum dalam berbagai aspek untuk mencari jawaban atas permasalahan yang telah dirumuskan dalam penelitian ini. Adapaun dalam penelitian ini penulis menggunakan tiga metode pendekatan antara lain pendekatan konseptual (*conceptual approach*), pendekatan perundang-undangan (*statute approach*), dan pendekatan kasus (*case approach*).

a. Pendekatan Konseptual (*Conceptual Approach*).

Pendekatan konseptual beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum. Dengan mempelajari pandangan-pandangan dan doktrin-doktrin di dalam ilmu hukum, peneliti akan menemukan ide-ide yang melahirkan pengertian-pengertian hukum. Pendekatan konseptual dilakukan guna dijadikan sebagai acuan untuk membangun argumentasi hukum yang berkaitan dengan pokok permasalahan dalam penelitian ini yakni mengenai pertanggungjawaban pidana atas rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia.

b. Pendekatan Perundang-Undangan (*Statute Approach*).

Pendekatan Perundang-Undangan dilakukan dengan menelaah semua Undang-Undang dan regulasi yang bersangkutan paut dengan isu karena yang akan diteliti adalah berbagai aturan hukum yang menjadi fokus sekaligus tema sentral suatu penelitian. Dilakukan dengan cara menelaah dan mengkaji semua peraturan perundang-undangan yang berkaitan dengan pokok permasalahan yang dirumuskan dalam penelitian ini. Pendekatan perundang-undangan ini digunakan untuk mendapatkan ketentuan-ketentuan hukum guna untuk mempelajari konsistensi dan kesesuaian antara Undang-Undang yang satu dengan Undang-Undang lainnya. Adapun pendekatan perundang-undangan dalam penelitian ini yakni Kitab Undang-Undang Hukum Pidana; Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik; Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi; Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta; Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

c. Pendekatan Kasus (*Case Approach*).

Pendekatan kasus (*case approach*) dalam penelitian hukum normatif merupakan metode pendekatan yang dilakukan dengan cara menelaah dan menganalisis kasus-kasus konkret yang telah diputus oleh pengadilan, khususnya putusan yang telah memiliki kekuatan hukum tetap (*inkracht van gewijsde*), untuk menemukan penerapan norma hukum dalam praktik. Melalui pendekatan ini, peneliti mengkaji pertimbangan hukum (*ratio decidendi*) hakim guna memahami bagaimana norma hukum ditafsirkan, diterapkan, dan dikembangkan dalam suatu putusan. Pendekatan kasus bertujuan untuk memperoleh argumentasi hukum, menemukan konsistensi atau inkonsistensi penerapan norma, serta mengidentifikasi adanya kekaburan norma, konflik norma, atau kekosongan hukum. Dalam penelitian ini pendekatan kasus yang digunakan terkait rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia.

1.7.3. Sumber Bahan Hukum (*Legal Sources*)

Bahan hukum yang dikumpulkan dalam penulisan untuk menjawab isu hukum penulisan ini yaitu: bahan hukum primer; bahan hukum sekunder; dan bahan hukum tersier.

1. Bahan Hukum Primer

Bahan Hukum Primer adalah bahan-bahan hukum yang mengikat seperti Norma dan Kaidah Dasar, Peraturan Dasar, Peraturan Perundang-Undangan. Bahan hukum primer yang digunakan adalah :

- a) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

- b) Kitab Undang-Undang Hukum Pidana;
- c) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik;
- d) Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi;
- e) Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta;
- f) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi;
- g) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; dan
- h) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan mengenai bahan hukum primer seperti : buku-buku hukum, hasil-hasil penelitian, pendapat pakar hukum. Dalam penelitian ini penulis menggunakan buku, makalah, hasil penelitian dalam bidang hukum, internet yang berkaitan dengan penelitian yang penulis lakukan.

3. Bahan Hukum Tersier

Bahan-bahan yang memberikan informasi tentang bahan hukum primer dan bahan hukum sekunder seperti : Ensiklopedia hukum, kamus bahasa Indonesia, kamus hukum, internet, hal ini dilakukan untuk mendukung dan menunjang penelitian penulis.

1.7.4. Teknik Pengumpulan dan Pengolahan Bahan Hukum

Berisi uraian logis prosedur pengumpulan bahan-bahan hukum primer, skunder, serta bahan hukum tersebut diinventarisasi dan diklarifikasi dengan menyesuaikan masalah yang dibahas. Dalam penelitian hukum normatif, teknik pengumpulan bahan hukum sebagai berikut:

Bahan hukum primer berupa perundang-undangan dikumpulkan dengan metode inventarisasi dan kategorisasi. Bahan hukum sekunder dikumpulkan dengan sistem kartu catatan (*card system*), baik dengan kartu ikhtiar (memuat ringkasan tulisan sesuai aslinya, secara garis besar dan pokok gagasan yang memuat pendapat asli penulis), maupun kartu ulasan (berupa analisis dan catatan khusus penulis).

Dalam penelitian hukum normatif yuridis, teknik pengumpulan bahan hukum sebagai berikut:

- 1) Bahan hukum priemer merupakan bahan hukum yang bersifat autoritatif artinya mempunyai otoritas. Bahan-bahan hukum primer terdiri dari perundang-undangan;
- 2) Bahan hukum sekunder berupa publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi. Publikasi tentang hukum

meliputi buku-buku teks, kamus-kamus hukum, jurnal-jurnal hukum, dan media daring.

1.7.5. Teknik Analisa Bahan Hukum

Analisis bahan hukum dalam penelitian ini berdasarkan data yang ada dilakukan secara yuridis kualitatif, yaitu tidak hanya mengungkapkan kebenaran belaka tetapi juga memahami kebenaran tersebut menurut aturan perundang-undangan. Dengan memberikan gambaran permasalahan tentang pertanggungjawaban hukum atas rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia dianalisis berdasarkan aturan hukum yang berlaku di Indonesia dan fakta di lapangan untuk kemudian diperoleh kesimpulan sebagai jawaban atas permasalahan yang diajukan.

1.8. Sistematika Penulisan

Untuk lebih mengetahui dan mempermudah dalam melakukan pembahasan, penganalisaan, dan penjabaran isi dari penelitian ini, maka dalam penulisan skripsi ini penulis menyusun sistematika penulisan sebagai berikut :

Bab I Menerangkan pendahuluan yang berisikan tentang latar belakang permasalahan, rumusan masalah, kajian pustaka, tujuan penelitian, manfaat penelitian, orisinalitas penelitian, kajian pustaka yang terdiri dari landasan teori dan penjelasan konsep, metode penelitian terdiri atas jenis penelitian, pendekatan masalah, sumber bahan hukum, teknik pengumpulan dan pengolahan bahan hukum, analisis bahan hukum, dan diakhiri dengan pertanggung jawaban sistematika.

Bab II Membahas mengenai pengaturan hukum positif di Indonesia dalam mengatur rekayasa konten digital berbasis kecerdasan buatan (*deepfake*). Dengan sub bab diantaranya: rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia; karakteristik tindak pidana konten digital berbasis kecerdasan buatan (*deepfake*); pengaturan hukum positif dalam mengatur rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia.

Bab III Membahas mengenai bentuk pertanggungjawaban hukum yang dapat dikenakan terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) di Indonesia. Dengan sub bab diantaranya: pertanggungjawaban hukum di Indonesia; pertanggungjawaban hukum terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) berdasarkan Undang-Undang Prorgografi; pertanggungjawaban hukum terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) berdasarkan Undang-Undang Informasi dan Transaksi Elektronik; pertanggungjawaban hukum terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) berdasarkan Undang-Undang Perlindungan Data Pribadi; pertanggungjawaban hukum terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) berdasarkan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; pertanggungjawaban hukum yang tepat diterapkan terhadap pelaku pembuatan dan penyebaran rekayasa konten digital berbasis kecerdasan buatan (*deepfake*) berdasarkan regulasi yang ada.

Bab IV Sebagai penutup berisikan beberapa kesimpulan dan juga saran dalam sebuah penelitian.