

BAB I

PENDAHULUAN

A. Latar Belakang

Kemajuan teknologi yang pesat menghadirkan beragam kemudahan terhadap kehidupan manusia. Namun, di balik manfaat tersebut, terdapat juga dampak negatif yang tidak dapat diabaikan. Di antaranya teknologi kecerdasan buatan yang dikenal dengan istilah *Artificial Intelligence (AI)*, yang membawa konsekuensi negatif yang kompleks, termasuk penyimpangan teknologi dalam kejahatan siber. Salah satu fenomena yang muncul akibat hal ini adalah *paradox of plenty*, yaitu kondisi di mana informasi sudah terlalu banyak sehingga sulit untuk menemukan informasi yang akurat. *Deepfake* merupakan salah satu contoh nyata dari fenomena *paradox of plenty* tersebut.²

Deepfake adalah salah satu bentuk dari kecerdasan buatan. Secara etimologis, istilah *deepfake* merupakan kombinasi dari kata *deep learning* dan *fake* dalam bahasa Inggris, di mana kata *fake* menggambarkan bahwa media yang dihasilkan bukanlah asli, melainkan bersifat rekayasa. Secara teknis, *deepfake* adalah teknologi *AI* yang digunakan untuk menciptakan foto, video, atau audio dengan tingkat kepercayaan tinggi. Teknologi ini dapat memodifikasi karakteristik wajah seseorang dengan teknologi kecerdasan buatan.³ Walaupun memiliki kegunaan dalam bidang industri kreatif,

² Jak101FM, "Mengenal Deepfakes, Teknologi AI yang Sering Digunakan untuk Menyebar Hoax," 2023, diakses dari <https://jak101fm.com/2023/10/mengenal-deepfakes-teknologi-ai-yang-sering-digunakan-untuk-menyebar-hoax/>

³ Nibert Young, *DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media* (New York: Independently Published, 2019).

pemanfaatan *deepfake* secara salah untuk menciptakan konten pornografi tanpa persetujuan telah mengakibatkan persoalan hukum yang signifikan. Dalam beberapa tahun terakhir, perubahan gambar atau video ini justru memberikan dampak yang lebih merugikan dibandingkan manfaat, khususnya bagi para korban penyebaran konten pornografi.

Survei pada tahun 2019 menunjukkan bahwa sebagian besar video *deepfake* yang beredar mengandung muatan pornografi, dengan presentase mencapai 96%.⁴ Beberapa tokoh publik, termasuk selebriti nasional, menjadi korban dari teknologi ini. Di Indonesia, kasus pornografi berbasis *deepfake* mengalami peningkatan dan berkaitan dengan pelanggaran terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi, serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Pasal 27 ayat (1) UU ITE melarang penyebarluasan informasi elektronik yang bertentangan dengan norma kesusilaan, sementara Pasal 4 ayat (1) Undang-Undang Pornografi menegaskan larangan atas pembuatan, penyebaran, dan penggunaan konten pornografi. *Deepfake* dapat menyebabkan dampak serius, seperti kerugian psikologis (kecemasan, ketakutan, depresi), kerugian sosial (merasa terpinggirkan dari lingkungan sekitar), serta kerugian ekonomi (kehilangan pekerjaan). Selain itu, kepercayaan korban terhadap penggunaan teknologi digital juga dapat menurun bahkan hilang sepenuhnya.⁵

⁴ Rahayu dan Santoso, "Analisis Gambar Wajah Palsu: Mendeteksi Keaslian Gambar yang Dimanipulasi Menggunakan Metode Variational Autoencoder dan Forensics Deep Neural Network," *Sibatik Journal*, hlm. 47

⁵ "Menggunakan AI Untuk Deepfake: Definisi, Dasar Hukum, dan Cara Mengatasinya," *BullyID*, diakses 21 Oktober 2025, <https://bullyid.org/edukasi-hukumtindakan-deepfake/>

Secara hukum, regulasi terkait *deepfake* masih menunjukkan ketidakjelasan karena meskipun sudah ada beberapa undang-undang yang selaras, banyak masyarakat yang belum mematuhi peraturan tersebut, bahkan sebagian masih melanggarnya. Sebagian undang-undang yang terkait dengan dampak *deepfake* di antaranya adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 yang telah diubah dengan UU Nomor 19 Tahun 2016 mengatur ketentuan mengenai informasi dan transaksi elektronik. Pasal 27 ayat (1) UU ITE melarang penyebaran informasi elektronik yang bertentangan dengan norma kesusilaan, sementara Pasal 4 ayat (1) Undang-Undang Pornografi menetapkan larangan terhadap pembuatan, pendistribusian, dan penggunaan konten pornografi. Selain itu, ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP), khususnya Pasal 378, 310, dan 311, serta pengaturan dalam Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Baru turut mengatur perbuatan tersebut. Dalam KUHP Baru, tindakan *deepfake* yang mengandung unsur penghinaan dan pencemaran nama baik dapat dikenakan sanksi pidana sebagaimana diatur dalam Pasal 433, 434, dan 436 juncto Pasal 441.

Pada tataran global, sejumlah negara telah merespons ancaman *deepfake* melalui kebijakan pemidanaan yang bersifat progresif, seperti beberapa negara bagian di Amerika Serikat yang menetapkan kriminalisasi terhadap penyebaran konten *deepfake* bermuatan politis atau seksual. Kondisi tersebut mencerminkan urgensi penyesuaian hukum pidana nasional agar mampu menghadapi ancaman yang bersumber dari kemajuan teknologi dan bersifat

lintas batas negara.⁶ Ketiadaan pengaturan hukum yang tegas dan terperinci mengenai kategori kejahatan menyebabkan proses penegakan hukum di Indonesia belum berjalan secara optimal. Penelitian ini menunjukkan bahwa aparat penegak hukum masih mengalami kendala dalam menentukan ketentuan pidana yang paling tepat untuk menjerat pelaku penyebaran deepfake. Akibatnya, banyak perkara *deepfake* yang tidak berlanjut hingga tahap persidangan, terutama karena hambatan dalam proses pembuktian.

Dari perspektif pertanggungjawaban pidana, penyebaran *deepfake* mengandung unsur kesengajaan (*mens rea*) yang dilakukan dengan tujuan merusak reputasi, menyebarkan konten pornografi, atau melakukan penipuan terhadap pihak lain. Dalam konteks kejahatan siber, pihak yang terlibat wajib mempertanggungjawabkan perbuatannya atas kerugian yang ditimbulkan. Pelaksanaan hak dan kewajiban hukum menuntut setiap individu untuk memikul tanggung jawab hukum atas setiap perbuatan yang dilakukannya. Melalui kebijakan hak cipta atas wajah dan suara warganya, Denmark berupaya menjamin bahwa penggunaan identitas wajah seseorang dalam konten *deepfake* tanpa persetujuan dapat dikenai sanksi hukum. Bahkan, Denmark memberikan perlindungan hak cipta atas wajah dan suara sebagai langkah preventif dalam mencegah penyalahgunaan *deepfake*, yang menunjukkan pendekatan pencegahan berbasis perlindungan privasi dan kekayaan intelektual. Di samping itu, pengembangan metode forensik digital yang efektif dalam

⁶C. Salvi, *Deepfake Evidence in Criminal Proceedings: Procedural Hurdles and Forensic Challenges* (2023), diakses dari <https://aiandcriminaljustice.uni.lu/wp-content/uploads/sites/260/2024/11/SALVI-8.711-Deepfake-evidence-Salvi-Crim-AI.pdf>

mengidentifikasi konten *deepfake* dengan tingkat ketepatan yang tinggi menjadi kebutuhan mendesak, mengingat keterbatasan alat bukti sering menempatkan korban dalam posisi yang rentan, sementara penegak hukum kerap mengesampingkan perkara semacam ini akibat kompleksitas dan tingginya biaya pembuktian. Negara memiliki kewajiban konstitusional untuk menghadirkan perlindungan hukum yang memadai agar kejahatan digital tidak tumbuh tanpa kendali hukum. Upaya tersebut dapat ditempuh melalui penyempurnaan peraturan perundang-undangan yang telah berlaku, sekaligus pembentukan regulasi khusus yang secara eksplisit mengatur kejahatan berbasis teknologi manipulatif, termasuk *deepfake*.

Perlindungan hukum harus diberikan bukan hanya ditujukan kepada korban tindak pidana, melainkan juga terhadap pelaku tindak pidana, agar pelaku memperoleh hukuman yang tetap menghormati hak fundamental. Proteksi hukum merepresentasikan peran hukum bagian dari instrumen yang menjamin keadilan, ketertiban, kepastian hukum, serta ketenteraman dalam kehidupan bermasyarakat. Pengaturan hukum yang tidak secara khusus dan spesifik mengatur tentang korban menyebabkan korban tidak mendapatkan perlakuan yang adil maupun hak atas kerugian yang dialaminya. Dalam perumusan kebijakan hukum, negara berkewajiban memastikan terwujudnya kepastian hukum serta perlindungan yang setara terhadap hak asasi manusia, baik dalam ketentuan pidana yang bersifat umum maupun khusus, guna memelihara ketertiban dan rasa aman di tengah masyarakat. Posisi individu sangat terkait dengan penggunaan teknologi di dunia maya. Dengan demikian, perumusan

kebijakan hukum perlu ditempatkan sebagai faktor utama dalam pembentukan ketertiban sosial, mengingat kemajuan teknologi merupakan unsur yang tidak terpisahkan dari kehidupan sosial masyarakat.⁷ Kebijakan yang dimaksud merujuk pada kebijakan hukum yang berorientasi pada perlindungan hak-hak korban. Korban berhak memperoleh berbagai hak, meliputi hak atas perlindungan, hak untuk mendapatkan pendampingan, hak memperoleh ganti rugi, serta hak untuk turut berpartisipasi.

Sudut pandang hukum Islam, penggunaan teknologi *deepfake* menimbulkan pertanyaan mendasar terkait dengan kebenaran, kejujuran, dan perlindungan martabat manusia. Sebagai agama yang berlandaskan pada nilai kebenaran dan keadilan, Islam memiliki prinsip-prinsip yang jelas dalam mengatur perilaku manusia, termasuk dalam menghadapi kemajuan teknologi. Konsep *al-haqq* (kebenaran), larangan *al-kadhib* (dusta), serta perlindungan terhadap karamah *al-insan* (martabat manusia) menjadi landasan utama dalam menilai legalitas penggunaan teknologi *deepfake*. Selain itu, prinsip *Maqashid Syariah* yang berfokus pada perlindungan agama, jiwa, akal, keturunan, dan harta. memerlukan evaluasi menyeluruh terhadap dampak teknologi ini demi kemaslahatan umat. Perspektif *Maqashid Syariah* sangat relevan untuk melengkapi kajian perlindungan hukum bagi korban *deepfake*, tidak hanya berfokus pada regulasi positif, tetapi juga pada nilai-nilai etika dan moral yang esensial dalam menjaga kehormatan dan keadilan di era digital.

⁷ Budi Sastra Panjaitan, *Viktimologi: Pandangan Advokat Terhadap Perbuatan Pidana dan Korban* (Banyumas: CV. Amerta Media, 2022), 6.

Sejalan dengan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji secara komparatif bentuk perlindungan hukum bagi korban *deepfake* berdasarkan ketentuan Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta meninjaunya melalui perspektif *Maqashid Syariah*. Melalui pendekatan tersebut, Penelitian ini diharapkan dapat merumuskan rekomendasi hukum yang bersifat lebih komprehensif, berkeadilan, serta selaras dengan nilai-nilai etika dan moral dalam merespons tantangan kejahatan digital di era modern.

B. Rumusan Masalah

Berdasarkan konteks penelitian diatas, maka rumusan masalah penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana perlindungan hukum dalam korban *deepfake*?
2. Bagaimana komparasi Undang-Undang ITE Nomor 19 Tahun 2016 dan Kitab Undang-Undang Hukum Pidana?
3. Bagaimana perlindungan hukum dalam perspektif *Maqashid Syariah*?

C. Tujuan Penelitian

1. Untuk mengetahui dan memahami bentuk perlindungan hukum terhadap korban *deepfake*
2. Untuk menganalisis komparasi antara Undang-Undang ITE Nomor 19 Tahun 2016 dan Kitab Undang-Undang Hukum Pidana
3. Untuk menganalisis perlindungan hukum terhadap korban *deepfake* dalam perspektif *Maqashid Syariah*

D. Kegunaan Penelitian

1. Kegunaan Teoritis

Penelitian ini memberikan kontribusi terhadap pengembangan ilmu hukum, khususnya di bidang hukum pidana dan hukum Islam. Melalui perbandingan Kitab Undang-Undang Hukum Pidana dan Undang-Undang Informasi dan Transaksi Elektronik dalam konteks perlindungan korban *deepfake*, penelitian ini dapat mengungkap sejauh mana regulasi yang ada mampu menangani kejahatan digital yang semakin kompleks. Penelitian ini juga menawarkan perspektif baru dengan meninjau dari sudut pandang *maqashid syariah* sebagai tujuan syariat Islam yang berorientasi pada penjagaan agama, kehidupan, akal, keturunan, dan harta. Penelitian ini tidak hanya membahas aspek hukum positif di Indonesia, melainkan juga mengaitkannya berdasarkan nilai moral dan etika dalam ajaran Islam. Temuan penelitian ini diharapkan dapat dijadikan sebagai landasan atau referensi mengenai kejahatan berbasis teknologi, khususnya *deepfake*.

2. Kegunaan Praktis

Secara praktik penelitian ini bermanfaat bagi beberapa pihak, antara lain:

a. Bagi Aparat Penegak Hukum

Hasil penelitian ini diharapkan memberikan kemudahan bagi aparat penegak hukum, seperti kepolisian, kejaksaan, dan hakim, dalam memahami dasar hukum yang tepat untuk menangani kasus *deepfake*. Aparat penegak hukum kerap menghadapi kendala dalam mengusut

tuntas perkara *deepfake* menghadapi tantangan yang lebih besar karena proses pengumpulan bukti dan identifikasi pelaku jauh lebih rumit dibandingkan dengan kasus pornografi konvensional. Kendala tersebut semakin diperparah oleh kemampuan teknologi *deepfake* yang memungkinkan pelaku menyembunyikan identitasnya, sehingga proses pelacakan hingga penegakan hukum menjadi semakin sulit.⁸ Dengan melakukan kajian komparatif terhadap ketentuan KUHP dan UU ITE, aparat penegak hukum diharapkan lebih cermat dalam menentukan pasal yang tepat serta mampu mengurangi potensi kekeliruan dalam penerapan hukum.

b. Bagi Pemerintah dan Pembuat Kebijakan

Penelitian ini dapat dijadikan rujukan dalam penyusunan atau revisi peraturan yang berkaitan dengan kejahatan digital, khususnya *deepfake*. Pemerintah sangat perlu melakukan perbaikan, pembaruan, atau bahkan merancang aturan baru untuk menangani peningkatan kasus *deepfake*, terutama yang berkaitan dengan pornografi. Pengaturan hukum mengenai pemanfaatan teknologi kecerdasan buatan, khususnya algoritma *deepfake*, memiliki urgensi tinggi dalam menjaga kerahasiaan data pribadi, mengingat teknologi tersebut merupakan bentuk kemajuan yang berdampak langsung terhadap perlindungan informasi personal. Di samping itu, regulasi tersebut diperlukan untuk memberikan perlindungan kepada masyarakat serta mengurangi risiko

⁸ Damarjati, "Fenomena Deepfake dan Tantangan Hukum Siber di Indonesia," *Jurnal Hukum dan Teknologi Informasi* 5, no. 1 (n.d.): 194.

penyalahgunaan pemanfaatan kecerdasan buatan yang bersifat tidak bertanggung jawab dan melanggar norma etika.⁹ Pandangan *maqashid syariah* memberikan kontribusi etis dan moral, sehingga regulasi yang disusun tidak hanya bersifat represif, tetapi juga bersifat preventif serta berfungsi menjaga kehormatan dan martabat manusia.

c. Bagi Masyarakat Umum

Penelitian ini berpotensi meningkatkan kesadaran hukum masyarakat tentang risiko dan dampak penyalahgunaan teknologi *deepfake*. Dengan memahami perlindungan hukum yang ada, masyarakat akan lebih waspada saat mengakses, menyebarkan, atau memproduksi konten digital. Dalam menghadapi tantangan penggunaan *deepfake* di kalangan remaja, peran orang tua dan guru sangat penting untuk memberikan bimbingan dan pengawasan terhadap penggunaan teknologi oleh mereka. Pendekatan yang diterapkan tidak boleh hanya bersifat represif dengan melarang penggunaan teknologi, tetapi juga harus bersifat edukatif dengan memberikan pemahaman mendalam mengenai konsekuensi moral dan hukum dari setiap tindakan digital.¹⁰

d. Bagi Korban *Deepfake*

Penelitian ini memberikan informasi dan panduan mengenai langkah-langkah hukum yang dapat diambil oleh korban *deepfake*.

⁹Zenifa Siti Hafsyari et al., "Korban Deepfake Pornografi: Evaluasi Efektivitas Hukum Positif dan Kebutuhan akan Reformasi Hukum," *Medium*, accessed August 13, 2024, <https://pleadsfhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitashukum-positif-dan-1fb2bb20da35>

¹⁰ Harianti, "Peran Orang Tua dalam Mengatur Penggunaan Gadget pada Anak Usia Dini," *Kumara Cendekia*, n.d.

Dengan menguraikan pasal-pasal dalam KUHP dan UU ITE, korban dapat memahami haknya serta prosedur hukum yang dapat dijalankan. Selain itu, pendekatan *maqashid syariah* memberikan dukungan moral dengan menegaskan bahwa perlindungan hukum bagi korban sesuai berdasarkan asas keadilan dan kemaslahatan dalam Islam.

E. Penegasan Istilah

1. Studi Komparasi

Studi komparatif digunakan sebagai pendekatan analisis hukum dengan cara membandingkan dua perangkat peraturan hukum, yakni Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Perbandingan tersebut bertujuan untuk menelaah persamaan, perbedaan, serta menilai kelebihan dan kekurangan masing-masing regulasi untuk melindungi korban *deepfake* secara hukum.¹¹ Studi komparasi juga diterapkan untuk menilai efektivitas kedua instrumen hukum tersebut dalam menghadapi tantangan perkembangan kejahatan digital di Indonesia, sekaligus mengevaluasi kesesuaian keduanya dengan prinsip-prinsip *maqashid syariah*.

2. Perlindungan Hukum

Perlindungan hukum dalam penelitian ini mengacu pada segala bentuk upaya yang diberikan oleh negara, baik melalui hukum pidana maupun regulasi khusus seperti UU ITE, untuk menjamin hak-hak korban *deepfake*.

¹¹Titin Patikasari, *Pelindungan Hukum Bagi Korban Deepfake Pornografi (Studi Perbandingan Indonesia dan Korea Selatan)* (Skripsi, Fakultas Syariah dan Hukum, UIN Syarif Hidayatullah Jakarta, 2024), 4

Perlindungan tersebut dapat bersifat preventif, berupa langkah-langkah pencegahan melalui regulasi, edukasi, dan teknologi deteksi dini, maupun represif, berupa sanksi pidana dan penegakan hukum terhadap pelaku kejahatan digital. Perlindungan hukum juga meliputi pemulihan hak korban dari segi psikologis, sosial, dan ekonomi agar korban memperoleh keadilan dan kepastian hukum. Saat ini, pengaturan mengenai perlindungan korban *deepfake* pornografi tersebar dalam sejumlah ketentuan peraturan perundang-undangan yang saling berkaitan, mengingat kejahatan tersebut mengandung unsur konten seksual sekaligus penyalahgunaan data pribadi. Tindakan ini dapat dikategorikan sebagai tindak pidana siber karena memenuhi unsur-unsur yang diatur dalam hukum positif Indonesia.

Peraturan hukum yang berlaku hingga kini masih belum memberikan daya ikat yang memadai untuk menindak pelaku, karena mengingat belum adanya aturan yang mengatur secara jelas dan menyeluruh terkait kejahatan *deepfake*, khususnya terkait dengan belum dicantumkannya istilah kecerdasan buatan atau *Artificial Intelligence* secara tegas tercantum dalam peraturan perundang-undangan. Selain itu, pengaturan mengenai tanggung jawab hukum dalam pemanfaatan teknologi kecerdasan buatan perlu dirumuskan secara jelas guna memberikan perlindungan kepada masyarakat, sekaligus menekan risiko yang ditimbulkan oleh penggunaan *AI* secara tidak etis dan tidak bertanggung jawab.¹²

¹² Zenifa Siti Hafsyari et al., “Korban Deepfake Pornografi: Evaluasi Efektivitas Hukum Positif,” *Medium*, diakses 13 Agustus 2024, <https://pleadsfhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake>

3. Korban *Deepfake*

Korban *deepfake* dalam penelitian ini merujuk pada seseorang maupun kelompok yang dirugikan akibat penyalahgunaan teknologi kecerdasan buatan (*Artificial Intelligence*) yang dimanfaatkan untuk memanipulasi wajah, suara, atau tubuh dengan tujuan yang melanggar hukum. Kerugian yang dialami korban meliputi kerugian psikologis seperti rasa takut, trauma, dan depresi, kerugian sosial seperti stigma, diskriminasi, dan hilangnya reputasi, serta kerugian ekonomi seperti kehilangan pekerjaan atau sumber penghasilan. *Deepfake* juga dapat memberikan dampak serius apabila korban menjadi sasaran ujaran kebencian, menghancurkan reputasi mereka karena dianggap melanggar norma oleh masyarakat, serta menurunkan atau bahkan menghilangkan kepercayaan korban dalam menggunakan teknologi digital.¹³ Dalam banyak kasus, korban *deepfake* kebanyakan adalah perempuan yang menjadi target konten pornografi tanpa izin, meskipun tidak menutup kemungkinan korban juga berasal dari kalangan publik figur, tokoh politik, maupun masyarakat umum.

4. Kitab Undang-Undang Hukum Pidana (KUHP)

Dalam konteks penelitian ini, KUHP dipahami sebagai hukum pidana materiil yang berlaku di Indonesia, yang mencakup KUHP lama (*Wetboek van Strafrecht*) serta KUHP baru sebagaimana diatur dalam

¹³Menggunakan AI untuk Deepfake: Definisi, Dasar Hukum, dan Cara Mengatasinya,” *BullyID*, diakses 21 Oktober 2025, <https://bullyid.org/edukasi-hukumtindakan-deepfake/>

Undang-Undang Nomor 1 Tahun 2023, yang memuat ketentuan pidana terhadap perbuatan pembuatan deepfake. Pengaturan tersebut tercantum dalam Pasal 407, yang melarang setiap orang melakukan tindakan mulai dari membuat, memproduksi, menggandakan, hingga menyebarkan, menyiarkan, mengimpor, mengekspor, memperjualbelikan, menyewakan, atau menyediakan konten bermuatan pornografi. Pelanggaran terhadap ketentuan ini diancam dengan ancaman pidana penjara paling singkat 6 bulan hingga paling lama 10 tahun, serta pidana denda mulai kategori V sebesar Rp200.000.000,00 sampai kategori VI sebesar Rp2.000.000.000,00. Namun, perlu diperhatikan bahwa KUHP baru ini akan mulai berlaku tiga tahun setelah diundangkan, yaitu pada tahun 2026.¹⁴ KUHP dijadikan sebagai dasar analisis karena mengandung ketentuan umum mengenai kejahatan yang berkaitan dengan kasus *deepfake*, seperti pencemaran nama baik, penghinaan, penipuan, serta penyebaran konten yang merugikan pihak lain. Dalam penelitian ini, KUHP dipahami sebagai kerangka hukum pidana umum yang dapat diterapkan untuk menindak oknum *deepfake*, meskipun istilah *deepfake* itu sendiri belum secara eksplisit tercantum dalam ketentuan tersebut.

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

Ketentuan UU ITE yang menjadi rujukan adalah Pasal 27 ayat (1), yang berkaitan erat dengan perlindungan data pribadi sebagai bagian dari

¹⁴ Ni Kadek Dwi Ika Ardiyani, "Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif," *Jurnal Kajian Hukum dan Kebijakan Publik* 2, no. 1 (Juli–Desember 2024): 607, <https://jurnal.kopusindo.com/index.php/jkhkp>

hak asasi manusia. Undang-Undang ITE digunakan sebagai dasar hukum dalam penanganan perkara *deepfake* pornografi yang beredar melalui media internet. Pemilihan ketentuan ini didasarkan pada karakter UU ITE yang secara spesifik mengatur aktivitas di ruang digital, termasuk larangan terhadap penyebaran informasi elektronik yang mengandung muatan kesusilaan, pornografi, serta pencemaran nama baik. Merujuk pada pasal tersebut, setiap orang yang dengan sadar dan tanpa hak mendistribusikan, mentransmisikan, atau membuat informasi dokumen elektronik yang memuat pelanggaran kesusilaan dapat diberikan sanksi pidana.¹⁵

Selanjutnya, Pasal 27A UU ITE memiliki peran penting sebagai pelengkap Pasal 310 KUHP. Meskipun unsur-unsur keduanya pada dasarnya serupa, Pasal 27A UU ITE menegaskan unsur tambahan terkait teknologi elektronik tanpa mengubah norma hukum pidana umum.¹⁶ UU ITE menjadi relevan karena banyak kasus *deepfake* terjadi melalui media sosial dan platform digital. Dalam penelitian ini, UU ITE dipandang sebagai instrumen hukum yang lebih khusus dibandingkan KUHP dalam mengatasi kejahatan berbasis teknologi.

6. *Maqashid Syariah*

Maqashid Syariah merupakan tujuan fundamental dari syariat Islam yang ditetapkan untuk menjamin dan memelihara kemaslahatan manusia

¹⁵ L. Heru Sujamawardi, "Analisis Yuridis Pasal 27 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik," *Dialogia Iuridica: Jurnal Hukum Bisnis dan Investasi* 9, no. 2 (April 2018): 89.

¹⁶"DPR: Ketentuan Pidana dalam UU ITE Diatur dalam KUHP Nasional," *Mahkamah Konstitusi Republik Indonesia*, diakses 31 Januari 2024, <https://www.mkri.id/index.php?page=web.Berita&id=19637>

melalui perlindungan atas lima unsur inti, meliputi agama, jiwa, akal, keturunan, dan harta.¹⁷ Pada kajian ini, *maqashid syariah* digunakan sebagai batasan istilah dan kerangka konseptual untuk memahami analisis perlindungan hukum terhadap korban *deepfake*, tanpa memasuki perdebatan teoretis yang lebih luas.

¹⁷ Abu Ishaq al-Shatibi, *Al-Muwafaqat fi Usul al-Shari'ah*, Juz II (Beirut: Dar al-Kutub al-'Ilmiyyah), hlm. 8–10.